San Francisco Police Department

Forensic Services Division

Request for Proposal-

Automated Biometric Identification System

Section 02 – Technical Specifications

March 31, 2009

TABLE OF CONTENTS

[THIS PAGE INTENTIONALLY LEFT BLANK]

1   INTRODUCTION

The San Francisco Police Department (SFPD) Forensic Services Division (FSD) Automated Biometric Identification System (ABIS) Request for Proposal (RFP) Technical Specifications volume is comprised of this Adobe PDF document including appendices and the requirements document (SFPD ABIS TRFP-Requirements.doc) that provide:

- An overview of the existing technical infrastructure impacting this procurement, including a description and diagrams of data workflow and current / planned systems
- An Operational Concept (OPSCON) of the envisioned Automated Biometric Identification System (ABIS) and related ABIS-centric applications with a set of General Requirements that apply to all Contract Line Items (CLINs)
- Specific Operational Concept (OPSCON) for each CLIN and set of Specific Requirements for the corresponding CLIN.

SFPD-FSD intends to select one or more vendors for initial project implementation and support contracts for up to five years, and options to continue support contracts for a period of up to five years each, which the City may exercise in its sole absolute discretion.

1.1   BUILDING TOWARDS AN END-VISION

SFPD is developing an End-Vision for a comprehensive and holistic Criminal Identity Management (C-IdM) infrastructure including a set of business processes and software applications that delivers services across the SFPD enterprise and to key stakeholders in the San Francisco Government (SFGOV). This C-IdM End-Vision infrastructure will include a suite of identity 'tools' delivered to the enterprise via a Services Oriented Architecture (SOA) leveraging primarily web services that drive a set of identity-centric engines that perform specific identity functions. A major portion of this C-IdM End-Vision infrastructure is a new ABIS.

In addition, SFPD is driving all user applications be delivered via an Enterprise Service Bus (ESB) topology as a part of this C-IdM End-Vision to ensure high availability and high reliability, flow-based transformation and routing, easier service-to-service communications and a flexible transport layer. A subset of these applications are 'ABIS-centric', in another words, a subset of these applications rely heavily on, or interact heavily with, the ABIS and leverage, at least in the near term, fairly straightforward read-only (application-to-system or system-to-system) interfaces to other internal identity-related data systems (such as CAD, JMS, RMS, Mugshot System, etc.).

In the future, SFPD anticipates the completion of the Justice Information Tracking System (JUSTIS) centralized SOA / ESB hub envisioned to interconnect the various Sheriff, Police, District

Attorney, Public Defender, Adult Probation, Juvenile Probation and Status of Women data management / IT systems and applications to allow sharing of criminal justice information across the law enforcement and community environment.

Although SFPD and the SFGOV are focused on a holistic and comprehensive technical and business process refresh for managing criminal identities as well as other law enforcement and prosecutorial information, FSD has a specific responsibility to replace the existing Automated Fingerprint Identification System (AFIS) with a robust multi-modal, multi-use ABIS that can easily fit into and interoperate with the End-Vision, including the JUSTIS SOA and ESB hub architecture currently being implemented by San Francisco (Department of Telecommunications and Information Services (DTIS)).

FSD has also identified specific ABIS-centric applications that are predicted to have significant benefits for SFPD, stakeholders and citizens as a whole.

As described in Business RFP Volume (Section 01), the components of the ABIS that have been identified as nearer-term priorities have been separated into discrete CLINs, depicted below (Figure 1) and described in detail in 4 - Specific Requirements located in this document.
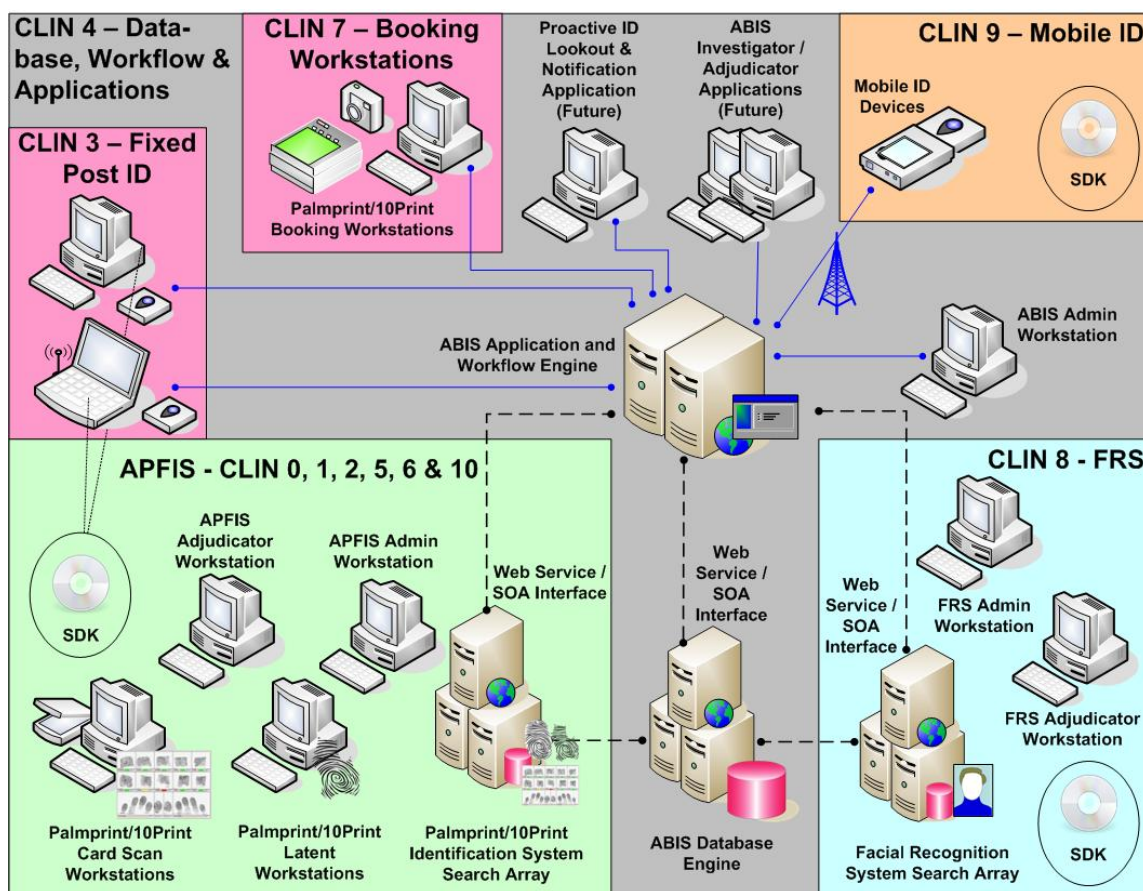
Figure 1 - ABIS components identified by SFPD as nearer-term priorities. Additional components will be added as needed in the future.

The goal of FSD is to implement these nearer-term ABIS components in such a way as to not only comply with SFGOV IT policies, goals and objectives (developed by the Committee on Information Technology (COIT)), but also enable SFPD to scale, upgrade or add new components as needed going forward in the most cost-effective way. The desired implementation will provide SFPD will future flexibility and avoid ties to proprietary solutions or technology.

In addition, the ABIS must support dynamic workflows, new applications, enhanced functionality, data translation and transformation as well as ever-changing interface formats and standards demanded by both internal (SFGOV) and external stakeholders (CAL-DOJ, FBI, WINS, Interpol, etc.) (Figure 2) In another words, the ABIS must be extensible.
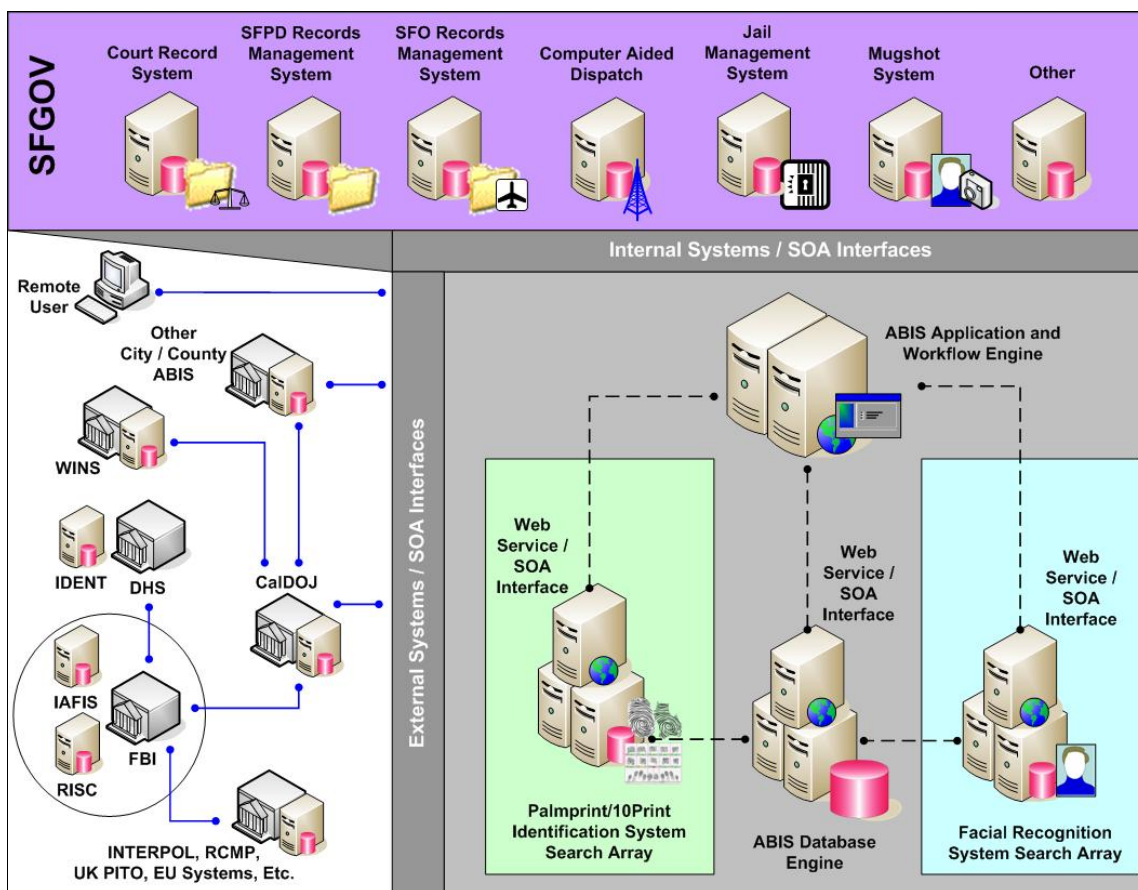
Figure 2 - The ABIS, and certain ABIS components, must be able to interface with other internal (SFGOV) systems, as well as interface with external stakeholder systems without relying on any one single vendor.

2   OVERVIEW OF EXISTING SYSTEMS

SFGOV has many stakeholders (e.g. agencies, departments, etc.) that leverage core identity and identity-related information, systems, applications and services, all of which are instrumental to the criminal justice process. Figure 3 below highlights some of the key SFGOV systems (and corresponding agencies/departments) shown in violet, and also depicts how the new ABIS will eventually integrate into the new SOA / ESB architecture (HUB) and related systems currently being delivered by SFGOV DTIS (shown in red).
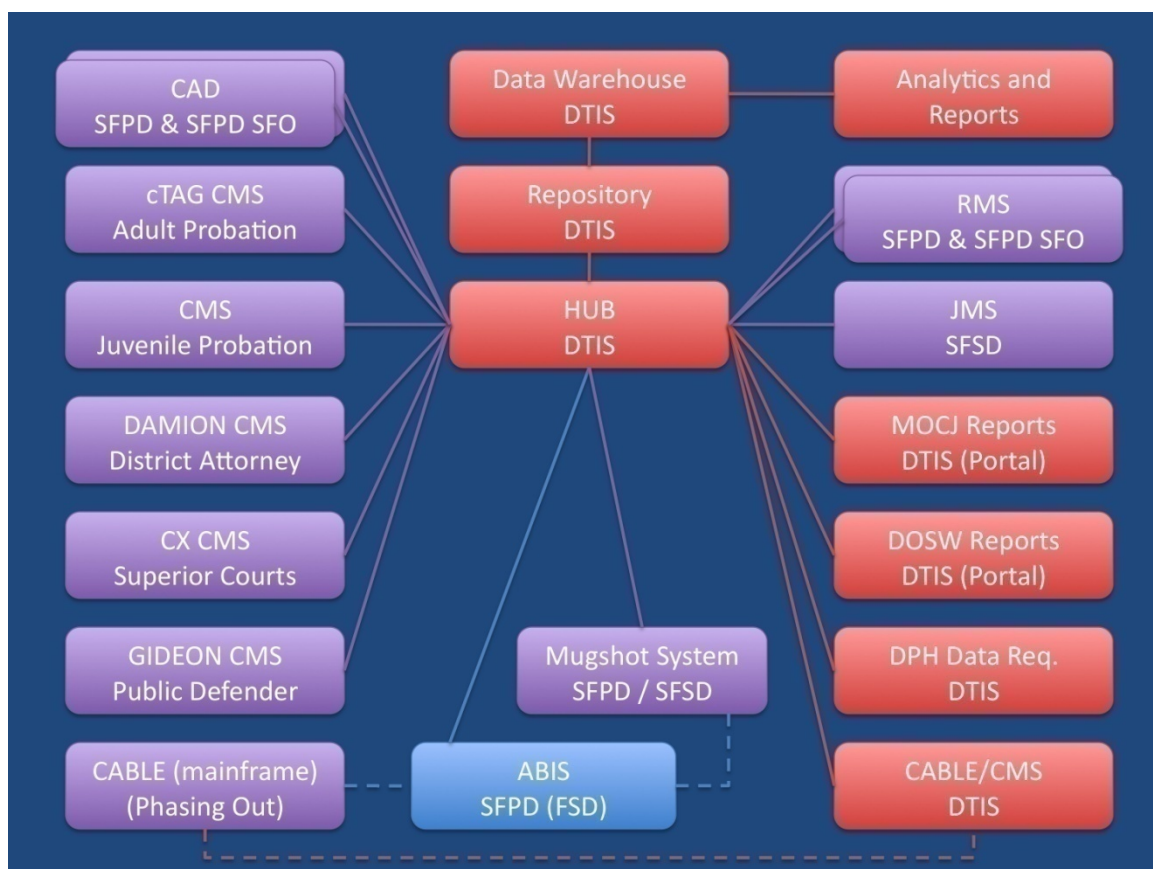
Figure 3 - Notional diagram depicting how identity-relevant systems may integrate with the new ABIS (both immediately and through the future SOA / ESB HUB architecture).

Please notice the direct interfaces between the ABIS and the existing CABLE mainframe system and the DataWorks Plus Mugshot System (shown as blue dashed lines). These will be explained in greater detail under the specific CLIN requirements.

A description of each system already existing or currently being installed follows:

Agency System	Vendor, Version No.	Description
Computer Assisted Bay Area Law Enforcement (CABLE)	Homegrown mainframe system first developed in 1975	CABLE is currently the master repository for all criminal information for SFPD and is where the SF Number (primary index) for each person-record is generated and managed.
Replacement CABLE System – Consolidated Management System (DTIS CABLE/CMS)	Homegrown solution built on Oracle.	The new Consolidated Management System (under development) is an aggregate of information from many systems across SFGOV including a wholesale import of all data from the existing CABLE system. New applications are being built on top of Oracle to deliver functionality to all stakeholder agencies and departments.
Existing SFPD Computer Aided Dispatch (SFPD CAD)	Tiburon CAD-2000 (www.tiburoninc.com)	The Hall of Justice communications facility uses Tiburon's CAD-2000 Computer Aided Dispatch System, running on a Stratus server and used windoze-95 for the four-quadrant, single-monitor CAD display. It is the same CAD software in use at Emergency Communications Department (ECD), except it does not have the full GUI display. The radio consoles are Motorola Centracom-II and operate on Low Band VHF (mobile radios) and on UHF (portable radios). The telephone system consists of the Lifeline 100 ANI/ALI controller; a B.C.S. Central Office switch and Positron Integrated Call Management call

		transfer units. The TDD interface equipment is made by Zetron. San Francisco Police Communications, as the County's P.S.A.P. (Public Safety Answering Point) receives 3500 to 4000 (TBD) calls for service each day, depending on the season.
SFO Computer Aided Dispatch (SFPD SFO CAD)	Intergraph (www.intergraph.com)	The Airport Bureau of SFPD has implemented their own, local dispatch system to enable interaction with airport communications and security management.
SFPD Records Management System (SFPD RMS)	New World Systems Aegis Law Enforcement Records Management (RMS) Version:7.9.2061 (to be upgraded to version 8.x after initial deployment is stable to version 8.x) (www.newworldsystems.com)	The new SFPD RMS (under development) will serve as the primary repository of criminal records, incident reports, etc.
SFPD Airport Records Management System (SFPD SFO RMS)	Intergraph iLeads RMS (www.intergraph.com)	The Airport Bureau of SFPD has implemented their own RMS to manage specialty crimes and international populations, and to interact with airport management systems. As of December 25 2008, the SFPD SFO RMS was managing 36,337 incidents (LWMAIN) and 73,271 names (NMMAIN).
SFSD Jail Management System (SFSD JMS)	New World Systems Aegis Corrections	The SFSD JMS has been implemented, will be receiving a software update and then will be

	Management (www.newworldsystems.com)	rolled out.
Adult Probation Case Management System (cTAG CMS)	Syscon Justice Systems (www.syscon.net)	This system is based on Oracle 8i and Crystal Reports and includes the following modules: • Case Intake and Discharge • Court Orders and Requests • Case Management • Programs and Services • Financial Obligations Tracking • Paper File Tracking • Workload Management • Imaging
Juvenile Probation CMS	JJIS (Juvenile Justice Information System) in-house application written in 1998 in Visual Basic 6, SQL Server 2000 Database back end, Crystal Reports 8.5 for all reports writing.	This is the main Criminal tracking system for Juvenile Probation. It was converted from the CABLE system in 1998 (when Juvenile Probation was part of CABLE). The original tables were: Detention, Contact, Petition, Dispositions, Person, Address, Offenses. Modified since with features such as: MugShot integration with SFPD, Document Management with Probation Services to include facesheets, social reports, detention reports, etc., Placements (group homes and foster home), Alternative to Detentions, Crime Location, and more tables (significant other, ID, Alerts, etc.). Currently working on a web-based user interface to integrate it with Microsoft Office SharePoint Server 2007 (MOSS). Plan to use Visual

		Basic.NET 2008, SQL Server 2005, Crystal Reports XI and Microsoft Reporting Services for report writing.
District Attorney Case Management System (DAMION CMS)	Constellation Justice Systems (www.damion.com)	This system is a browser-based system based on Oracle 8i and Crystal Reports and includes the following modules: • Case Tracking with event status, next event, etc. • Case Assignment and Management Functions for attorneys and task forces • Legal Document production • Log of Correspondence, Legal Briefs • Database journaling to track changes made in case files Interface with Microsoft Office templates Standard Reporting and Ad Hoc Reporting
Existing Superior Court Case Management System (Court CMS)	Home grown system in Microsoft Access; conducting procurement for COTS product(s)	Builds all FSD casework and administrative worksheets, tracks evidence and supplies modules not covered by the SFPD RMS.
Replacement Superior Court Case Management System (Court CX/CX 2000)	CX Corporation (www.cx2000.com)	The new Case Management System (under development).
In-Car Data Systems and Communications	Data911 Touch Screen Mobile Computers (www.data911.com)	9.6kbps voice and data going to 56kbps voice and data connection. SFO vehicles have 2G/3G wireless cellular modem cards installed.

2.1   EXISTING AFIS

SFPD has operated its own stand-alone AFIS since the mid 1980's. The original system, an Advanced Computer Operating System (ACOS) based AFIS from NEC®, the first to be installed in North America, has been upgraded several times. In 2000, the AFIS was migrated to the NEC AFIS21® platform. In addition, several Positive ID® (PID) devices were added in order to provide an automated pre-booking / intake identification capability at the city's district police stations and county jail. In 2001 the system was upgraded to a UNIX/NT platform. In 2002, an automated palm print matching capability was added to the system.

Today the department operates 6 AFIS21 Workstations, including:

AFIS21 Client	Quantity	Location
Tenprint Scan	2	1 in ID Section and 1 in CSI AFIS Room
Tenprint + Palmprint Scan	1	1 in ID Section
Latent Scan	3	3 in CSI AFIS Room

For current system sizing and metrics, see Appendix B – ABIS Metrics.

For detailed system and workflow diagrams, see Appendix C – Diagrams and Workflows.

2.2   LIVESCAN WORKSTATIONS

SFPD / SFSD currently operates four varieties of Livescan workstations:

Livescan Model	Captures	Quantity	Locations
Identix® TouchPrint™ 2000	Rolled Fingerprints Slap Fingerprints	3	• Superior Court (Hall of Justice at 850 Bryant Street) • SFSD (Main Jail at 425 7th Street)

			• SFO Airport Bureau (SFO Airport) a. Applicant print processing
Identix TouchPrint 3000	Rolled Fingerprints Slap Fingerprints	1	• San Francisco State University (`1600 Holloway Ave`) o Applicant print processing

Identix TouchPrint 3800	Rolled Fingerprints
	
	Slap Fingerprints
	
	Full Hand Prints
	
	Writer's Palm Prints
		9	• Three (3) systems located at SFPD ID Bureau (Room 475, Hall of Justice at 850 Bryant Street)
			
			   a. One system is for applicant print processing
			
			• One (1) at SFSD (Main Jail at 425 7th Street)
			
			• One (1) at Juvenile Justice Center (475 Woodside Ave)
			
			• One (1) at Community Assessment and Referral Center (121 Leavenworth Street)
			
			• One (1) at US Park Service (1217 Ralston Avenue)
			
			• One (1) at SF Parks and Recreation Police (501 Stanyan Street)
			
			   a. Applicant print processing
			
			• One (1) at SF Human

			Services (44 Gough Street) a. Applicant print processing

Biometrics4All® LS300 Software with Cross Match® L Scan Guardian® Devices	Rolled Fingerprints
	
	Slap Fingerprints
	
	(Linked to DNA per CA Proposition 69 – 296 DNA)
		6	• Five (5) systems are installed at SFSD jail facilities (in-custody processing)
			
			  a. 850 Bryant Street
			
			  b. 425 7th Street
			
			  c. San Bruno Facility
			
			• One (1) system is installed at a central collections site (out-of-custody processing)
			
			  a. 425 7th Street

All booking and applicant Livescan systems operate through three (3) Identix store-and-forward servers. Two (2) Identix store-and-forward systems located in room 475 at the Hall of Justice (ID Bureau) processes all criminal and registrant transactions. A single (1) store-and-forward server located on the 5th floor at the Hall of Justice processes all applicant transactions.

The following LSID's are currently transmitting through the 2 Store-and-Forward Servers on the 4th floor. These records are transmitted to the existing local AFIS and then on to CalDOJ:

- 217
- 218
- 220
- 616
- A36
- B25
- E99
- X14

The following LSID's are currently transmitting their records through the Application Store-and-Forward on the 5th floor: (All of these records transmit directly to Cal DOJ)

- 221
- 222
- 224
- A55
- MX1

The Biometrics4All LS300 workstations currently connect directly to CalDOJ for DNA Livescan functionality required by California Proposition 69. The Boimetrics4All LS300 workstations are used after the booking process is complete to positively link one or more DNA samples collected from the corresponding individual to the booking/ID record previously enrolled.

2.3   EXISTING MUGSHOT SYSTEM

The existing system is a DataWorks Plus® Digital PhotoManager™ image system leveraging a SQL database. SFGOV has an existing contract with DataWorks Plus for maintenance of hardware and software. Approximately 564,988 photos exist on the image bank fileserver. The ^{system} presently is handling 3 capture stations and WebWorks Plus™/WebWorks Express™. Components include:

- Digital PhotoManager™ Server Edition
- Digital PhotoManager™ Client Edition
- WebWorks™ Server Edition
- WebWorks Plus™ for 3 Concurrent Users
- WebWorks Express™ for 10 Concurrent Users
- One (1) Share File Interface with RMS (XML)
- LiveScan Interface

The SFGOV mugshot system, as with other DataWorks Plus systems throughout the state, is connected to a larger DataWorks Plus system located in Sacramento, CA that collectively makes up the majority of mugshots available through CAL-Photo.

2.3.1   PHOTO-CAPTURE STATIONS

At SFSD jail facilities, the prisoner arrest number (SF#) is entered prior to photographing the prisoner to pull down (retrieve) arrest data from the JMS. At all capture stations have the ability to operate in a stand-alone mode if there is a communication failure with the mainframe. In this situation, prisoner data can be manually entered. Upon recovering from stand-alone mode, the photo-imaging records saved during this period are automatically updated.

2.3.1.1 RETRIEVAL STATIONS

Searches can be performed to find a specific person or they can be randomized based on a description. Photographs and pedigree information can be viewed or printed. Line-ups, wanted flyers, mugshot profiles are available in this function.

3　GENERAL REQUIREMENTS

The General Requirements includes subheadings and content that shall be considered the set of mandatory technical requirements which apply to all CLINs including details regarding the scope of implementation and operation, system features and functions, system acceptance procedures, training requirements and required level of ongoing support and maintenance. These mandatory General Requirements are detailed in the attached document (SFPD ABIS TRFP-Requirements.doc). This document includes "General Requirements" (CLIN = ALL) that lists the detailed mandatory (M) General Requirements for all CLINs.

As described in the Business RFP Volume, Section 01 with respect to the evaluation and proposal scoring process, bidders may choose to include additional optional or desirable (D) features and functions that are identified in SFPD ABIS TRFP-Requirements.doc.

3.1.1　SCOPE OF IMPLEMENTATION AND OPERATION

3.1.1.1 SYSTEM SOLUTION

1. The bidder shall provide all software, hardware, equipment and accessories (e.g. network switches, racks, cables, uninterruptible power supplies, backup hardware/software/consumables, etc.), professional services (e.g. installation, training, support, etc.), documentation (e.g. training guides, user guides, administrator guides, troubleshooting guides, installation instructions, specification sheets, etc.) and tools that will be required to implement, train, operate (initially), support and maintain each CLIN:
    1) In accordance with manufacturers' requirements and recommendations for that CLIN, and;
    2) In accordance with all General and Specific Requirements specified for the corresponding CLIN (included in this document).
2. SFGOV agencies, divisions and bureaus will NOT provide any software, hardware, equipment, accessories, professional services, documentation or tools required to implement, train, operate (initially), support or maintain (initially) any CLIN, except where indicated within this document.
3. Bidder shall describe, for each CLIN proposed, how the component or solution is aligned with the following strategic plans, programs and related standards and guidelines:
    3.1. CalDOJ Vision 2015
    3.2. CLETS 2008 Strategic Plan
    3.3. Cal DOJ Latent Print Section Strategic Planning
    3.4. FBI Next Generation Identification (NGI)
    3.5. FBI Information and Technology Branch Strategic Planning

3.6. FBI Laboratory Services Strategic Planning

3.7. NIST/NIJ Latent Interoperability and Information Sharing Mandate

3.1.1.2 DETAILED LISTING AND DESCRIPTIONS

4. The bidder shall provide a complete and comprehensive listing and description (i.e. a Bill of Materials (BOM) of all software, hardware, equipment and accessories (e.g. network switches, racks, cables, uninterruptible power supplies, backup hardware/software/consumables, etc.), professional services (e.g. installation, training, support, etc.), documentation (e.g. training guides, user guides, administrator guides, installation instructions, specification sheets, etc.) and tools that will be included in bidder's proposal to implement, operate (initially), support and maintain each proposed CLIN in compliance with all manufacturers' requirements and recommendations.

5. Bidder shall specify any software, hardware, equipment and accessories, professional services, documentation and tools that will NOT be transferred to SFGOV after system acceptance as a part of the final contract.

3.1.1.3 FACILITY COMPLIANCE

6. The bidder shall have the opportunity to examine all facilities where proposed software, hardware, equipment and accessories are to be installed during the bidder's tour that will be conducted in conjunction with the bidder's conference.

    6.1. The bidder is responsible for identifying any physical space (size, mounting, etc.), HVAC, power, communications (network, remote dial in capabilities, etc.) or any other facility constraints or issues at any or all of the facilities that may impact the ability to install, operate, support or maintain a given CLIN in compliance with all manufacturers' requirements and recommendations.

7. The bidder shall provide a recommendation on how SFPD or SFGOV may upgrade, replace or rectify one or more facilities' constraints to accommodate the proper installation, operation, support and maintenance of the proposed CLIN in compliance with all manufacturers' requirements and recommendations.

    7.1. If the bidder does not identify any facility constraints or issues for a given CLIN within their proposal, SFPD will assume that the bidder has either 1) not found any constraints or issues for the implementation or operation of the proposed CLIN in compliance with all manufacturers' requirements and recommendations; or 2) included the cost of upgrading, replacing or rectifying one or more facilities' constraints or issues to accommodate the proper installation, operation, support and maintenance of the proposed CLIN in compliance with all manufacturers' requirements and recommendations.

3.1.2 SYSTEM FEATURES AND FUNCTIONS

1. These <u>mandatory</u> General Requirements for System Features and Functions for all CLINs are detailed in the attached document (SFPD ABIS TRFP-Requirements.doc). This document lists the detailed <u>mandatory</u> (M) General Requirements for all CLINs.

2. As described in the Business RFP Volume, Section 01 with respect to the evaluation and proposal scoring process, bidders may choose to include other optional or desirable features and functions that are detailed in the requirements document. The Desired or Optional requirements are identified with a (D). Each bidder may want to consider including in their proposal for a given CLIN.

3. Bidder shall describe how their product(s) and solution(s) utilize COTS application, workflow and database servers both 1) internally to accomplish the capability and 2) externally to interact with other systems, applications and services.

4. Bidder shall describe how their product(s) and solution(s) both adhere to and integrate with a Web 2.0 infrastructure / architecture

3.1.3 STANDARDS COMPLIANCE

1. Bidder shall specify any and all industry, American and international standards compliance and/or certifications that the software, hardware, equipment and accessories, professional services, documentation and tools hold for each proposed CLIN.

2. Bidder shall indicate, specify, highlight and discuss any and all standards, certifications and best-practices specific to the identity management, biometrics and credentialing industry, as well as, relevant electrical/electronic hardware, software, SOA, ESB, web services, security, access control and security standards that will be adhered to in each proposed CLIN. Some of these standards and standards bodies have been listed below as a courtesy (there may be other standards and standards bodies that are relevant that are not listed here):

   2.1. ANSI/NIST ITL and FBI EFTS / EBTS (EBTS XML) Biometric Data File Formats

   2.2. FBI's IAFIS Image Quality Specifications and Certification Standards

   2.3. WSQ Fingerprint Image Compression Encoder/Decoder Certification Standards

   2.4. Global Justice and NIEM XML File Formats

   2.5. ANSI, ISO and ICAO Biometric Quality Assurance, Storage and Template Standards

   2.6. NIST Information Access Division Image Group - Mobile ID Device Best Practice Recommendation

   2.7. NIST/NIJ Latent Interoperability and Information Sharing Mandate

   2.8. International Association for Identification (IAI) Standards, Guidelines and Best Practices

   2.9. Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Standards, Guidelines and Best-Practices

   2.10.   Best practices resulting from research NIST is conducting on the usability of biometrics (Biometrics and Usability Website from NIST)

   2.11.   NIST Best Practice Recommendation for Capture of Mugshots

   2.12.   INCITS/L3 - Coding of Audio, Picture, Multimedia, and Hypermedia Information

   2.13.   ISO TC42 (Photography)

2.14.   (ISO) Joint Photographic Experts Group, JPEG, and Joint Bi-level Image experts Group, JBIG

2.15.   NIST FIPS 201 Credentialing / Biometric Standards

2.16.   ICAO Travel Document and Biometric Standards

2.17.   ANSI and ISO Smart Card Standards

2.18.   ANSI, ISO and AAMVA Card / ID Standards

2.19.   OASIS Biometric Identity Assurance Services (BIAS)

2.20.   OASIS Biometric Standards for the Financial Industry (e.g. X9.84)

2.21.   International Standard Framework for Identity Management - US International Committee for Information Technology Standards (INCITS CS1), which serves as the US Technical Advisory Group to ISO/IEC JTC1, and also under Category C Liaison status directly with ISO JTC1 SC27.

2.22.   SFPD/SFGOV, FBI CJIS, Cal-DOJ and NIST Security and Access Control Standards, including but not limited to:

   2.22.1. SFPD/SFGOV Security and Access Control Policies and Procedures

   2.22.2. FBI CJIS Security Policy v4.4

   2.22.3. FBI CJIS Security Policy v5.0 (DRAFT as of the release of this RFP)

   2.22.4. CLETS Policies, Practices, and Procedures (PPP) – October 2008

   2.22.5. Security Requirements for Cryptographic Modules (FIPS PUB 140-1 / 140-2)

   2.22.6. Role Based Access Control and Role Based Security (INCITS 359-2004 RBAC and INCITS CS1.1)

   2.22.7. Enterprise Telework and Remote Access Security (SP 800-46 and SP 800-46 Revision 1)

   2.22.8. Recommended Security Controls for Federal Information Systems and Organizations (SP 800-53 Revision 2 and SP 800-53 Revision 3)

   2.22.9. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (SP 800-122)

   2.22.10.   Recommendation for EAP Methods Used in Wireless Network Access Authentication (SP 800-120)

   2.22.11.   Electronic Authentication Guideline (SP 800-63 and SP 800-63 Revision 1)

   2.22.12.   Digital Signature Standard (DSS) (FIPS 186-2 and FIPS 186-3)

   2.22.13.   Recommendation for Key Management (SP 800-57)

   2.22.14.   Guidelines on Cell Phone and PDA Security (SP 800-124)

   2.22.15.   Guide to General Server Security (SP 800-123)

   2.22.16.   Guide to Bluetooth Security (SP 800-121)

   2.22.17.   Guide to Storage Encryption Technologies for End User Devices (SP 800-111)

   2.22.18.   An Ontology of Identity Credentials (SP 800-103)

   2.22.19.   Guide to Secure Web Services (SP 800-95)

   2.22.20.   Guide to Computer Security Log Management (SP 800-92)

2.22.21.   Guide to Malware Incident Prevention and Handling (SP 800-83)

2.23.   SOA, ESB, Web Services, Federated Processes and XML/JSON Processing Standards

2.23.1. Web 2.0 Architectures, Standards and Best-Practices

2.23.1.1.   REST, SOAP Web APIs

2.23.2. OASIS, ISO/IEC, Liberty Alliance, World Wide Web Consortium (W3C), The Open Group, Open Grid Forum

2.23.2.1.   XML

2.23.2.2.   Messaging

2.23.2.3.   Metadata Exchange

2.23.2.4.   Security

2.23.2.5.   Privacy

2.23.2.6.   Reliable Messaging

2.23.2.7.   Resources

2.23.2.8.   Web Services Interoperability

2.23.2.9.   Business Process

2.23.2.10. Transaction

2.23.2.11. Management

2.23.2.12. Presentation

2.24.   Hardware, electronic and electrical

2.24.1. Federal Communications Commission Part 15 Certification

2.24.2. Underwriter's Laboratory (UL) Compliance

2.24.3. European Union CE Certification

2.24.4.   ISO / IEEE standards and best practices

2.25.   Software development and business process/management standards

2.25.1. ISO 9000/9001

2.25.2. Software Engineering Institute (SEI) Capability Maturity Model Integrated® (CMMI)

2.25.3. Project Management Institute® Project Management Body of Knowledge (PMBOK)

2.25.4. ITIL/ITSM

2.26.   Energy conservation and environmental (and technologically environmental friendly) standards, certifications and best-practices

2.26.1. State of California and SFGOV

2.26.2. US / Canada

2.26.3. ISO

2.26.4. EU

3.1.4 SYSTEM INSTALLATION

1. The bidder shall provide all software, hardware, equipment and accessories, professional services, documentation and tools required for the installation of each proposed CLIN.
2. The bidder shall identify any and all industry and professional standards, certifications, guidelines and best practices that will be followed by bidder for the installation of all software, hardware, systems, equipment and accessories included in a given CLIN.
   2.1. The bidder shall follow any and all industry and professional standards, certifications, guidelines and best practices required by SFGOV for the installation of all information technology (IT) software, hardware, systems, equipment and accessories. Bidder is responsible for researching, identifying, specifying and providing proof of compliance for any and all SFGOV standards, certifications, guidelines and best practices that apply.
   2.2. Bidder shall remain in compliance with all SFGOV, State of California and US Federal building codes.
3. SFGOV may elect to provide professional resources (e.g. qualified personnel, managers, consultants, etc.) to 'ghost' the bidder's installation and configuration team for educational, observational and compliance purposes only.
   3.1. SFGOV personnel will be instructed not to hinder or impede the expediency of the particular CLIN installation unless bidder is found to be non-compliant with the final contract for the corresponding CLIN.

3.1.5   SYSTEM ACCEPTANCE

1. Acceptance tests will be performed on each CLIN to determine if the system delivered under the CLIN meets the required and specified accuracy, throughput, functionality, interoperability, system fault tolerance, failover, backup & restore and other requirements specified here and in the Specific Requirements under the corresponding CLIN.
   1.1. These test plans shall be for all hardware, functionality and requirements including, but not limited to, all CLIN software, hardware, equipment and accessories as well as system processes (e.g. quality assurance, data workflows, etc.).
2. Bidder shall be present during the performance of each system acceptance test. In no way shall the bidder deviate from the systems acceptance test plan negotiated prior to final contract signing.
3. SFPD reserves the right to conduct additional tests at any time during the life of the contract.
4. SFPD will validate that all capabilities proposed by bidder for the corresponding CLIN have been delivered and operate correctly prior to system acceptance. Bidder shall participate in the validation process and will be notified immediately of any discrepancies.
5. This validation and system acceptance process is envisioned to last no more than 30 days for each CLIN.
6. The bidder shall work with SFPD to prepare and document validation and test plans for systems acceptance, including expected results and validation/testing techniques for accuracy, throughput, functionality, interoperability, backup & restore and all other

requirements. All plans must be approved by SFPD prior to acceptance testing and shall be contract deliverables.

7. The bidder shall perform all system acceptance validation/testing in accordance with the SFPD approved test plans.

8. SFPD will review the results of the validation and provide an acceptance or rejection letter signed by the proper SFPD authority and addressed to the bidder. Only after the bidder receives this SFPD acceptance letter will the CLIN be considered complete and accepted.

9. These test plans shall indicate what requirements will be validated in conjunction with the bidder prior to usage verses those requirements validated through daily usage by SFPD staff and personnel.

    9.1. SFPD plans to validate key specific requirements and functionality through normal usage during the first month.

10. The bidder shall provide a full and complete audit trail for all system acceptance validation / testing and the requisite reports from this audit trail.

3.1.6   SYSTEM OPERATIONS

1. The bidder shall provide all software, hardware, equipment and accessories; professional services (initially), documentation and tools required for proper CLIN operations.

2. Professional services (e.g. bidder personnel) for proper CLIN operations must remain on-site for a minimum of the first five (5) days of operations after system acceptance for the corresponding CLIN. After the first five (5) consecutive days of operations (after system acceptance), bidder can extract operational personnel. Once bidder extracts the bidder's operational personnel, the contracted CLIN system support begins.

3. While on-site, bidder's operational personnel will work closely with SFPD and SFGOV operational personnel to ensure optimal knowledge transfer. During this operational period, SFPD and SFGOV may require the CLIN system to experience exceptions and failures in order to ensure that SFPD and SFGOV operational personnel are completely trained and understand how to best deal with or recover from these exceptions.

4. The bidder shall describe how they plan to staff and support the first five (5) days of operations for each CLIN proposed.

5. The bidder shall describe all system fault tolerances, redundancy and failover to ensure 99.99% (4-nines) uptime for the proposed CLIN.

3.1.7   TRAINING

1. The bidder shall provide all software, hardware, equipment and accessories, professional services, documentation and tools required to train designated SFGOV and SFPD personnel for each proposed CLIN.

2. The bidder shall perform ongoing periodic training assessments to evaluate the effectiveness of bidder's training program.   Bidder shall recommend assessment intervals in their proposal.

2.1. The bidder shall make adjustments to the training program if the evaluation(s) indicated changes are required to improve the effectiveness of training.

3. Training reports shall be prepared by the bidder and delivered to SFPD no less frequently than weekly once the training program has begun.

4. The bidder shall provide an outline of the proposed training plan, including a description and timeline, for each proposed CLIN.

   4.1. The bidder shall provide a description of how, where and when the training of users, operators and/or administrators will take place, including what will be required of SFGOV or SFPD (e.g. access to facilities, access to students, student information, direction from managers, etc.) to ensure success.

   4.2. The training plan must identify the type(s) of training the bidder shall utilize for each CLIN proposed (e.g. Train-the-User/Operator/Administrator, Train-the-Trainer, Computer Based Training (CBT), Hands-On Training, Classroom Training, etc.)

   4.3. The estimated number of students for each CLIN is detailed in the Specific Requirements section of this document.

   4.4. Should the bidder's training plan include items not defined as required in this document but deemed necessary to fully understand the bidder's solution, that content shall be included.

   4.5. All schedules for training will be coordinated with and approved by the SFGOV/SFPD Project Manager.

   4.6. SFPD shall retain final approval authority for all training approaches and content.

5. The bidder shall provide all curriculum (instructional guides, master presentations, videos, charts, graphs, diagrams, etc.), learning aides (computers and software, white boards, overhead projectors, calculators, reference books, etc.) and student materials (instructional books, user and administrator guides, troubleshooting guides, presentation material, pens, pencils, paper, etc.).

6. Electronic and hard copies of all curriculum (instructional guides, master presentations, videos, charts, graphs, diagrams, etc.) and student materials (instructional books, user and administrator guides, troubleshooting guides, presentation material, etc.) shall be provided to SFGOV/SFPD to assist current instructors and students during CLIN system operations and support, as well as future instructors and students trained by SFGOV/SFPD instructors.

   6.1. Electronic copies shall not be protected by passwords and shall be in an original file format such that all file or document elements can be manipulated and modified by SFSFGOV/SFPD, including the ability to copy, cut and paste. For example, all diagrams must be provided in an original file format that can easily be edited and manipulated by SFGOV/SFPD personnel.

   6.2. Bidder shall also provide all curriculum and all student materials in a searchable and indexed Adobe Acrobat PDF format.

7. The bidder shall directly train designated SFGOV/SFPD instructors for each CLIN proposed. SFGOV/SFPD instructors may be comprised of select internal personnel and managers, designated subcontractors including officers and staff located at the SFPD Academy.

7.1. Bidder shall provide 'train-the-trainer' professional services for a maximum of three (3) SFGOV/SFPD qualified personnel per CLIN proposed.

8. The bidder's instructors shall have extensive knowledge of the software, hardware, systems, processes, etc. for each proposed CLIN, including any and all 3rd party software, and be prepared to answer questions from students immediately or within 24 hours of the time the question is asked.

9. The bidder shall provide training during normal, daily business hours (Pacific Standard Time) on Monday through Friday.

9.1. SFPD's daytime shift operates from 7:00 AM to 7:00 PM daily.

10. The bidder shall provide formal training, as needed or requested, for any and all upgrades made to software, hardware or systems.

11. The bidder shall train system users, operators, administrators and technical support staff.

12. The bidder shall provide Training in the following activities, to include but not be limited to:

12.1.1. Adding, removing users, changing user roles;

12.1.2. Statistical reporting on accuracy, reliability, throughput and productivity;

12.1.3. Managing administrative parameters;

12.1.4. Standard and ad hoc report design and preparation;

12.1.5. Problem / Error reporting, troubleshooting and recovery;

12.1.6. System traffic monitoring;

12.1.7. Main console operations;

12.1.8. Systems security;

12.1.9. Database management and maintenance (including database configuration, optimization, tuning, maintenance, diagnostic tools, alerts and routines);

12.1.10.   System performance monitoring tools;

12.1.11.   Managing batch jobs and ad-hoc requests;

12.1.12.   Backup and restore operations;

12.1.13.   Server operation and basic maintenance;

12.1.14.   Workstation operation and basic maintenance;

12.1.15.   Peripheral operations and basic maintenance; and

12.1.16.   Interface operations and basic maintenance.

3.1.8   DOCUMENTATION

1. Bidder shall provide the following documentation in soft copy (PDF) format on a CD/DVD disc and at least one (1) hard copy bound in a professional binder using double-sided color printing:

1.1. Installation and Set-Up Guide

1.2. Configuration, Tuning and Optimization Guide

1.3. Routine Maintenance and Cleaning Guides

1.4. Administrator's Guide

1.5. Troubleshooting Guide (for Level 1 support at a minimum, Level 2 support preferred)

1.6. User's / Operator's Guide

1.7. Developer's Guide (for all web services, Software Development Kits (SDKs) and all products delivered in CLIN 4)

1.8. Source Code Guide (for all applications and systems interfaces that require the transfer of source code to SFPD)

3.1.9 SUPPORT AND MAINTENANCE

1. The bidder shall provide all software, hardware, equipment and accessories, professional services, documentation and tools required to support designated SFGOV and SFPD personnel and/or software, hardware, equipment and accessories included in each proposed CLIN.

2. Bidder shall provide level 1, level 2 and level 3 support and software maintenance for the first 12 months from the date of system acceptance for each proposed CLIN. SFPD/SFGOV exclusively retains the option of extending any and all support and/or software maintenance beyond the first 12 months after the date of systems acceptance for each proposed CLIN.

    2.1. The bidder shall describe the various standard support packages offered to existing customers for each proposed CLIN (e.g. bronze, silver, gold, platinum, etc.), including bidder's definition of level 1,2 and 3 support, a description of the various guaranteed response times, experience, location and certification of support staff, availability and inventory levels of spare hardware, equipment and accessories, etc.

    2.2. SFGOV/SFPD personnel will serve as daily users, operators and administrators of each proposed CLIN. SFGOV/SFPD also desires to be self-sustainable with the ability to provide basic technical support (at a minimum) for each proposed CLIN leveraging users/operators/administrators and/or existing or new technical employees (or consultants) that support one or multiple CLIN systems and/or other existing SFGOV/SFPD systems.

        2.2.1. Basic technical support is defined as routine maintenance, tuning and optimization, basic troubleshooting as prescribed in bidder's troubleshooting guides, performing failover, backup and recovery functions, dealing with basic system failures, answering technical questions from users, operators and administrators, etc.

    2.3. The bidder shall provide qualified support via telephone/mobile phone, email, instant messaging, file transfer (FTP), remote system dial-in and facsimile to supplement and assist SFGOV/SFPD support staff (including consultants) for each proposed CLIN.

        2.3.1. Bidder shall provide qualified support staff knowledgeable in all basic and intermediate components, functions, features, workflows, etc. of the corresponding proposed CLIN.

        2.3.2. Bidder shall provide qualified support staff that fluently speaks the English language, including any and all technical terms.

        2.3.3. Bidder shall ensure that the level 1 support staff remain engaged in the support request (as a facilitator or coordinator) regardless if the incident/case is escalated to level 2 or level 3

2.4. The bidder shall provide all level 2 and level 3 support to SFGOV/SFPD as an incident or case escalates above level 1 support status.

2.5. The bidder shall describe all software maintenance, updates (major verses minor), bug fixes, patches, etc. offered either in standard support packages or via standard software maintenance fees.

4   SPECIFIC REQUIREMENTS

Each CLIN includes major subheadings and content that should be considered the entire CLIN deliverable and set of mandatory Specific Requirements including detail regarding the scope of implementation and operation, system features and functions, system acceptance procedures, training requirements and required level of ongoing support and maintenance.   These mandatory Specific Requirements are detailed in the attached document (SFPD ABIS TRFP-Requirements.doc).

The following increments are defined for delivery and operational capability. The corresponding Contract Line Item Number (CLIN) is included in each major subheading as a courtesy.

4.1   CLIN 0 – DIGITIZATION OF INKED CARD DATA

4.1.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**

2. SFPD requires that a collection of inked cards be digitized (scanned) so the data can be loaded into the new Automated Palmprint and Fingerprint Identification System (APFIS) (CLIN 1 and 2), comingled with Livescan data and checked for aliases and to compare against unsolved latent prints.

3. Palmprint and Ten-print cards are of the FBI and CAL-DOJ standard format and size of 8 inches x 8 inches.

4. Approximately 400,000 Ten-print cards shall be digitized by the bidder. Approximately 150,000 Palmprint cards shall be digitized by the bidder.

4.1.2   SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.

2. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 0" for mandatory requirements.

3. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 0" for desired requirements.

4.1.3   STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

2. Bidder shall only implement scanning hardware and software that are listed on the FBI master listing of certified scanning systems/devices.[1] SFPD reserves the right to inspect all hardware and software to ensure model and part numbers match those indicated on letters of certification issued by the FBI.

3. Bidder shall only implement JPEG2000 image compression algorithms that have been certified by the FBI. SFPD reserves the right to request a certified copy of the certification letter from the FBI and require bidder to demonstrate the installed JPEG2000 algorithm matches the algorithm indicated on the certification letter.

4. Bidder shall only implement systems that store the resultant digitized images and alphanumeric text in an ANSI/NIST and/or FBI compliant file format. Bidder shall specify which version of the ANSI/NIST/FBI standard will be used to store all data, for example:

    4.1. ANSI/NIST-ITL 1-2007[2]

    4.2. ANSI/NIST-ITL 2-2008 (XML)[3]

    4.3. FBI Electronic Fingerprint Transmission Specification (EFTS) 7.1[4]

    4.4. FBI Electronic Biometric Transmission Specification (EBTS) 8.x[5]

    4.5. FBI EBTS XML Information Exchange Packet 8.x[6]

5. Bidder shall include NIST-ITL-2007 Type 9 data with the M1-378 block (which adheres to the conventions defined and described by the ANSI INCITS 378-2004 standard. Annex G of the standard contains detailed descriptions of the fields used for the M1-378 features together with the required conventions and parameters).

4.1.4   SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

2. The bidder shall provide all facilities required to house all scanning equipment.

3. Bidder shall only implement scanning hardware and software that are listed on the FBI master listing of certified scanning systems/devices.[7]

4. Bidder shall provide SFPD a NIST/FBI EFTS/EBTS viewing, sorting, text searching and printing application to enable easy viewing and printing of scanned data (images and text) from flat files or a database.

    4.1. Bidder shall provide a description of the image file search, retrieval, viewing, text-searching and printing application.

---

[1] http://www.fbi.gov/hq/cjisd/iafis/cert.htm

[2] http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

[3] http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf

[4] http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[5] http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

[6] http://www.fbibiospecs.org/fbibiometric/docs/EBTS-8001-XML_Draft1.zip

[7] http://www.fbi.gov/hq/cjisd/iafis/cert.htm

4.2. Bidder should specify if the application is stand-alone, connects to a common database or is an add-on module to another CLIN.

4.1.5 SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.
2. Bidder shall process ten (10) Ten-print and ten (10) Palmprint cards.
3. Bidder shall display the results on-screen and demonstrate that all images are in the proper location and orientation with minimal cropping or clipping of the images.
4. Bidder shall demonstrate all images are 1000ppi in resolution and 8-bits in grayscale shades.
5. Bidder shall demonstrate all images are compressed using a FBI-certified JPEG2000 algorithm at a compression ration of no more than 15:1.
6. Bidder will demonstrate file format meets or exceeds FBI and NIST standards.
7. Bidder will print out the same twenty (20) cards and demonstrate the images match the original cards

4.1.6 SYSTEM OPERATIONS

1. See **System Operation** under **General Requirements**.
2. The bidder shall provide a secure courier service to move Ten-print and Palmprint cards in lots from SFPD facilities to bidder-provided facilities for processing and upon completion of processing.
3. SFPD and bidder will work together to determine how many cards will be in each lot to optimize processing while minimizing the impact to SFPD operations.
4. Bidder shall identify any and all cards that experience errors when scanning (including missing, distorted, damaged, clipped, cropped, etc. images) via a comprehensive scanning report that includes SF#, ROI#, TCN#, Person's Full Name, a description of the error(s) encountered and how the error(s) were rectified or overrode.

4.1.7 TRAINING

1. See **Training** under **General Requirements**.
2. Bidder shall provide designated SFPD personnel a detailed description and in-person review of the final data files (or database) delivered to SFPD.
3. Bidder shall train designated SFPD personnel on the NIST/FBI EFTS/EBTS image file search, retrieval, viewing, text searching, sorting and printing application.

4.1.8 SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.
2. Bidder shall propose a warranty to SFPD to cover the re-scanning of any cards found to be improperly or inadequately scanned by bidder.
3. Bidder shall propose support and maintenance options for the NIST/FBI EFTS/EBTS image file search, retrieval, viewing, text searching, sorting and printing application.

4.2   CLIN 1 – AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

4.2.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**
2. SFPD requires a next-generation AFIS to simultaneously enable multi-application functionality above and beyond traditional tenprint and latent processing resulting in higher transaction rates. Some of these already identified applications include Fixed Post ID (FPID - CLIN 3) and Mobile ID Pilot (MID - CLIN 9).
3. SFPD initially requires that 'Basic AFIS' capability be available for both ten-fingerprint and latent-fingerprint processing, as well as to support the FPID application and MID Pilot, both of which will utilize a subset of fingers from each individual for a rapid identification or verification.
4. Bidders shall describe how the new Basic AFIS will be implemented with training, systems acceptance and then brought on-line via a transition from the existing AFIS. Bidder shall also describe how tenprint, latent and then FPID and MID workflows, interfaces and applications will be configured and commissioned.
5. In order to facilitate rapid deployment, the bidder shall utilize SFPD provided electronic image databases to be supplemented with images scanned in CLIN 0. In addition, the initial Basic AFIS shall utilize an automatic encoding of the existing SFPD latent images to form the baseline Unidentified Latent File (ULF) (NOTE: this would be analogous to lights out latent-fingerprint processing). The ULF shall have the capability to have the automatic encoded latent fingerprints be supplemented with manual encodings, or electronically converted NEC-based encodings.
6. Bidder shall develop an interface with the existing mugshot system so that all booking records are linked to one or more mugshots (photos of face, scars, marks and tattoos).
   6.1. AFIS shall be able to retrieve mugshot images related to a given identification or verification transaction and include in the data payload that is sent back to the requesting workstation or system, including via web services.
   6.2. Bidder shall transfer all source code of mugshot interface to SFPD.
7. Bidder shall develop a 3290-terminal emulation interface with CABLE to retrieve SF# assigned to each individual at booking and insert into the AFIS with the corresponding record(s).
   7.1. SFPD will facilitate bidder access to IT specialists at SFGOV that manage CABLE to enable the building of the interface.
   7.2. Bidder shall transfer all source code of 3290 interface to SFPD upon AFIS system acceptance
   7.3. Interface shall leverage an 'auto fill in' and 'screen-scrape approach' to retrieving SF# assigned by CABLE to each booking record.
8. Bidder shall describe and propose palm print functionality / system via CLIN 2, if applicable.

4.2.1.1 BASIC AFIS

9. The Basic AFIS constitutes the electronically and manually converted Ten Print, the converted latent files for lights out processing, the hardware required for processing these files and the software and workflow to perform the searching of these files. The capabilities of the Basic AFIS shall be based upon commercial-off-the-shelf (COTS) systems. That is, each bidder shall be able to meet the mandatory General and Specific requirements with existing features and functions of bidder's COTS AFIS.

10. Bidder shall also indicate any and all non-mandatory (optional) requirements that bidder shall ship with bidder's COTS AFIS (the Basic AFIS – CLIN 1). The intent of this is to achieve very early deliverable of the Basic AFIS that meets the basic needs of SFPD including forward search for latents utilizing lights out latent searching.

11. CLIN 11 through 14 enables each bidder to bundle and propose additional non-mandatory requirements as customizations, modifications or supplied by a third party (see Appendix D).

4.2.1.2 AFIS ARCHITECTURE

12. Bidder shall describe how their COTS product can be implemented into an enterprise SOA / ESB architecture leveraging Web 2.0 compliant web services.

13. Bidder shall describe bidder's COTS AFIS architecture and how workflows and business rules are implemented in bidder's COTS AFIS.

14. Bidder shall describe bidder's AFIS workflow and rules engine and whether a proprietary or 3rd party (brand name) workflow engine is utilized. Bidder shall also describe if bidder's COTS AFIS workflows are static, dynamic and/or configurable by SFPD, and if so the level of corresponding difficulty.

15. For ten print processing, the bidder shall describe which identification (1:n and x:n) technique(s) shall be delivered in bidder's COTS AFIS. Examples of techniques include filtering using a biometric image-based index, 100% database penetration, fixed or variable number of fingers used in each search, etc.

    15.1.   Bidder shall not use any alphanumeric text (i.e. biographic or demographic information about the individual) to perform identifications.

4.2.1.3 AFIS ALGORITHM AND SYSTEM PERFORMANCE

4.2.1.3.1 ACCURACY

16. Bidder shall describe how SFPD can operate bidder's COTS AFIS at a target operational accuracy level of Equal Error Rate = 1×10^{-9} (0.0000001%).

17. Bidder shall provide copies of ALL accuracy results of testing conducted by the National Institute of Standards and Technology (NIST), including all tables, charts and graphs provided to bidder by NIST.

17.1.   Bidder shall organize NIST test results by 1) NIST test type / name and 2) by the bidder's algorithm identifier assigned by NIST and used in the NIST test. Bidder shall include test results from the following NIST tests if bidder participated:

17.1.1. Fingerprint Vendor Technology Evaluation (FpVTE)

17.1.2. Evaluation of Latent Fingerprint Technologies (ELFT and ELFT-EFS)

17.1.3. Slap Fingerprint Segmentation Evaluation (SlapSeg and SlapSegII)

17.1.4. Ongoing Proprietary Fingerprint Template Testing

17.1.5. Ongoing Minutiae Exchange Test (MINEX)

17.1.6. NFIQ Compliance Testing

18. Bidder shall specify and identify which algorithm(s) used in NIST testing shall be included in bidder's COTS AFIS proposed to be delivered to SFPD.

19. If the bidder participated in the testing for the Next Generation Identification (NGI) program conducted by the FBI and Lockheed Martin, and the test results are available for release to SFPD, bidder shall provide these test results organized by test type (10-print rolled, 10-print segmented slap, 2 finger, etc.). If these test results are not available, bidder shall indicate this in their proposal.

4.2.1.3.2 SPEED

20. Bidder shall propose a system speed for the COTS AFIS for all simultaneous transactions below based on metrics provided in Appendix B:

20.1.   Number of tenprint transactions per minute

20.2.   Number of latent fingerprint transactions per minute

20.3.   Number of FPID transactions per minute

20.4.   Number of MID transactions per minute

21. Bidder shall describe to SFPD how bidder, or a cited 3rd party, has measured algorithm and system speeds.

22. Bidder shall explain how SFPD can increase system speed in the future (e.g. by adding additional hardware, registering fewer records per server / blade, software/algorithm upgrades, etc.).

4.2.1.4 LATENT CAPABILITY

23. SFPD requires that all latent prints be processed as quickly as possible by the Basic AFIS and therefore requires bidder to implement lights out latent processing for all latents.

23.1.   Bidder shall implement lights out processing for the initial encoding and searching of the Unsolved Latent File (ULF).

23.1.1. Bidder shall propose an encoding and searching schedule of latent processing of the ULF that will not slow down the AFIS or overwhelm the latent examiners such that the processing of new daily latent cases is not impacted.

23.2.   Bidder should review CLIN 5 for the manual encoding and searching of the ULF and CLIN 6 for the electronic conversion of the ULF from the NEC format including subsequent searching.

24. Bidder shall enable the subsequent manual encoding (re-encoding) of all latents on a priority basis based on crime type, urgency or a specific need.
25. Latents will be searched against the tenprints producing a list of the top 10 candidates in highest score priority at a rate specified by SFPD (and configurable in the solution).
26. Bidder shall include a discussion of any expected benefit of incorporating reverse searching capability (Ten Prints against ULF) and all impacts upon system performance.
    26.1.   Bidder shall explain any resulting increase in identification rates and the rationale for this belief (including any data supporting this).

4.2.2   SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.
2. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 1" for <u>mandatory</u> requirements.
3. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 1" for <u>desired</u> requirements.
4. Bidder shall propose a system that can manage up to 1 million persons in the database and the transaction rates described in Appendix B (AFIS, Fixed Post ID, Mobile ID, etc.).
    4.1. Bidder shall describe any hardware, software, licensing or contractual conditions or restrictions that would prevent SFPD to register over 1 million persons in the system and operate at a reduced system speed (e.g. transaction rate, response time, etc.).
    4.2. Bidder shall describe how SFPD will be notified in advance prior to the system is reaching the 1M person-record limit.
5. Bidder shall describe how much database space (memory, hard drive space and table space) is required to store all relevant biometric data (images and templates), configuration data, event log and reporting data, backup/restore data, any workflow triggering or instruction set data, etc.
    5.1. Bidder shall remember that the most recent shipping version of either Oracle or SQL will be used by the bidder's system.
6. Bidder shall provide a Basic AFIS than supports mixed-resolution operations (both 500ppi and 1000ppi).
7. Bidder shall only implement systems that store the resultant digitized images and alphanumeric text in an ANSI/NIST and/or FBI compliant file format. Bidder shall specify which version of the ANSI/NIST/FBI standard will be used to store all data, for example:
    7.1. ANSI/NIST-ITL 1-2007[8]
    7.2. ANSI/NIST-ITL 2-2008 (XML)[9]
    7.3. FBI Electronic Fingerprint Transmission Specification (EFTS) 7.1[10]
    7.4. FBI Electronic Biometric Transmission Specification (EBTS) 8.x[11]
    7.5. FBI EBTS XML Information Exchange Packet 8.x[12]

---

[8] http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

[9] http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf

[10] http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[11] http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

[12] http://www.fbibiospecs.org/fbibiometric/docs/EBTS-8001-XML_Draft1.zip

8. Bidder shall provide an AFIS that supports and interfaces with Oracle or SQL persistent storage database delivered under CLIN 4. All AFIS records must be stored in this database.
   8.1. Proprietary database(s) can only exist inside the AFIS for the purposes of searching or matching fingerprints and for fail-over and redundancy.
9. Bidder shall include NIST-ITL-2007 Type 9 data with the M1-378 block which adheres to the conventions defined and described by the ANSI INCITS 378-2004 standard. (Annex G of the standard contains detailed descriptions of the fields used for the M1-378 features together with the required conventions and parameters).
10. Bidder shall enable system to support required workflow for SFPD operations, including criminal ten-fingerprint, civil/applicant ten-fingerprint, registrant ten fingerprint, FPID and MID two/four fingerprint and latent-fingerprint identification and verification processes
    10.1.   Bidder shall provide web service that supports all of these matching functions. Bidder shall describe functionality delivered in bidder's COTS AFIS web services.
11. Bidder shall deliver the following minimum functionality in the COTS AFIS
    11.1.   Latent searching selectable as manual or lights out processing (ULF search against Tenprint database)
    11.2.   Tenprint search against ULF database
    11.3.   Latent search against unsolved latent (ULF)
    11.4.   Tenprint identification and verification functionality
    11.5.   Two finger and four finger rapid identification and verification capability for FPID and MID applications.
    11.6.   Segmenting of multi-finger slap images
    11.7.   Best quality composite tenprint record per SF# as primary record plus multiple incident records including the five (5) most recent bookings, based on a configuration value within the solution.

4.2.3 STANDARDS COMPLIANCE
1. See **Standards Compliance** under **General Requirements**.

4.2.4 SYSTEM INSTALLATION
1. See **System Installation** under **General Requirements**.

4.2.4.1 DATA MIGRATION
2. Bidder shall migrate tenprint and latent data to the new AFIS.
   2.1. Bidder shall auto-encode all SFPD latent images for lights out searching.
   2.2. Bidder shall assume all digital images are 500ppi and in FBI/ANSI/NIST file format
   2.3. Bidder shall use the SF# for each record as a primary index for the AFIS database. Bidder shall use the CalDOJ# and FBI# as secondary indexes for the AFIS database.
   2.4. Bidder shall store all biographic data from each booking record in the AFIS database

3. SFPD will also request a complete set (copy) of image files transmitted by SFPD to CalDOJ in the past to be leveraged during the bidder's populating of the AFIS with existing records.

    3.1. Some of CalDOJ-provided records may not be on file at SFPD due to errors and omissions…however it is more likely that all DOJ-provided files will be a subset of the record set currently managed by SFPD.

    3.2. The records provided by CalDOJ may include updated fingerprint images (one or all) for the same subject/person that were captured by another agency in the state of California as an update to the record. If these prints are of a higher quality than those on file at SFPD for the same individual, the prints from CalDOJ shall be used.

    3.3. Bidder will work with CalDOJ to ensure data is in a format acceptable for use by bidder's COTS AFIS

4. SFPD anticipates a complete card conversion at 1000ppi as stipulated in CLIN 0 will be accomplished. The majority of these records have already been scanned at 500ppi previously and registered in the existing AFIS.

    4.1. The bidder shall import all newly converted cards and extract fingerprint minutiae data at 1000ppi. Any existing corresponding records at 500ppi will be updated with 1000ppi data.

    4.2. Bidder shall assume all digital images are 1000ppi and in FBI/ANSI/NIST file format

5. Bidder shall ensure that for all data that is migrated, bidder shall maintain complete data integrity and shall ensure that all privacy act requirements are met.

    5.1. For example, no data shall be lost, all data shall be converted properly, the pedigree of the data shall be tracked, original data shall not be altered and no data shall be mixed up or altered.

    5.2. To achieve this, the bidder must submit a Data Conversion and Migration Plan that addresses all of these issues for each type of data and demonstrates that the vendor will convert data properly.

6. Prior to migrating any data, SFPD will require that the bidder convert a set of sample data (records) for each file type that will be migrated.

    6.1. 20 complete files (for each file type) shall be selected by the SFPD and provided to bidder. Bidder shall convert/migrate these 20 files to the new Basic AFIS in accordance with the requirements specified.

    6.2. The converted/migrated files will be tested/evaluated by SFPD. If SFPD determines the conversion/migration to be acceptable, an approval document to that effect will be provided to the bidder prior to full data conversion/migration. Upon receipt of this document signed by a proper SFPD authority, bidder shall then perform the full migration/conversion of this particular file type.

4.2.4.2 DATA CLEANSING

7. Bidder shall perform a cleansing of all records in the database to 1) detect all duplicates and aliases; and 2) ensure the highest quality fingerprints are committed as a part of the primary/master record for each individual for future identification and verification purposes.

4.2.5   SYSTEM OPERATION

1.   See **System Operation** under **General Requirements**.

4.2.6   SYSTEM ACCEPTANCE

1.   See **System Acceptance** under **General Requirements**.

2.   Prior to system acceptance, the tenprint and latent accuracy requirements shall be tested to verify that the operational system achieves the same or better accuracies than what has been achieved by relevant NIST and/or FBI testing.

   2.1. Bidder shall recommend and describe a set of test protocols / test plan to satisfy this requirement.   SFPD reserves the right to review and approve all proposed test protocols and test plans.

   2.2. SFPD reserves the right to perform additional tests to verify that performance meets or exceeds the accuracies achieved by relevant NIST and/or FBI testing.

   2.3. After system acceptance, accuracy tests will continue to run on a regular basis to reconfirm system performance and detect any degradation.

3.   The tenprint response time requirements (AFIS speed) shall be verified on the Basic AFIS after the initial tenprint records have been loaded to that system and cleansed, and prior to system acceptance.

   3.1. A test group shall include a sample of transactions typical to SFPD operations including a statistically significant number of poor quality prints (approximately 3-5%). The bidder and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

   3.2. The test will be deemed successful if the results meet or exceed bidder's COTS AFIS response times proposed by bidder.

   3.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

4.   The latent response time requirements shall be tested on the COTS Basic AFIS after the initial ULF records have been loaded to that system, and prior to system acceptance.

   4.1. A test group will consist of varying image quality and size and shall include a sample of transactions typical to SFPD operations including cases with multiple lifts. The bidder and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

   4.2. The test will be deemed successful if the results meet or exceed bidder's COTS AFIS response times proposed by bidder.

   4.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

5.   The FPID and MID (two finger) response time requirements shall be tested on the COTS AFIS after the initial tenprint records have been loaded to that system and cleansed, and prior to system acceptance.

   5.1. A test group shall include a sample of transactions typical to SFPD operations including a statistically significant number of poor quality prints (approximately 3-5%). The bidder

and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

5.2. The test will be deemed successful if the results meet or exceed bidder's COTS AFIS response times proposed by bidder.

5.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

4.2.6.1 DATA MIGRATION

6. Bidder shall propose a set of system acceptance validations/tests that shall demonstrate the bidder has complied with the Data Conversion and Migration Plan. This set of system acceptance validations/tests, along with the Data Conversion and Migration Plan, must be approved by SFPD before any data migration occurs.

7. During/following conversion completion the vendor/SFPD shall perform the acceptance tests in the Data Conversion and Migration Plan. SFPD will review the acceptance plan results and provide an acceptance or rejection letter signed by the proper SFPD authority to the vendor. Only if the vendor receives the acceptance letter will the conversion be considered complete and accepted.

4.2.7   TRAINING

1. See **Training** under **General Requirements**.

2. The bidder shall train SFPD staff/trainers on all workstation activities, including, but not limited to:

2.1. Tenprint processing

2.2. Latent fingerprint processing

2.3. Image acquisition

2.4. Report requests

2.5. Record lookups

2.6. Updating and inserting target records

2.7. System / database administration, configuration, tuning and optimization

4.2.7.1 LATENT PRINT TRAINING

3. Training shall include, but not be limited to;

3.1. Latent fingerprint entry (use of camera, lighting techniques, use of scanner, calibration tools, search set-up, use of filters, use of printers, use of clarification tools, encoding of minutiae, marking of other print characteristics used by bidder);

3.2. Latent evaluation;

3.3. Latent verification;

3.4. ULF function;

3.5. Interoperability of entry and evaluation with CalDOJ State

3.6. Interoperability of entry and evaluation with the FBI/IAFIS including the Universal Latent Workstation (ULW) application

3.7. Latent image exporting and importing

4.2.7.2 TENPRINT TRAINING

4. Training shall include, but not be limited to:

4.1. ABIS Workstation functions,

4.2. Image acquisition and manipulation,

4.3. image encoding,

4.4. image manipulation,

4.5. data entry,

4.6. workflow,

4.7. validation,

4.8. verification,

4.9. minutiae placement,

4.10.   quality control,

4.11.   diagnostic routines,

4.12.   backup and recovery functions

4.2.8   SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.

4.3   CLIN 2 – PALMPRINT IDENTIFICATION SYSTEM

4.3.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**

2. Palmprint capability is not required for the Basic AFIS in the interest of rapid initial deployment, although it is desirable. The bidder may propose to deliver CLIN 2 with CLIN 1 with an explanation as to why such inclusion will not result in a slower initial deployment.

3. After Basic AFIS capabilities are accepted, the SFPD desires that Basic Palmprint capability be provided in the same manner as CLIN 1.

4. Bidders shall describe how palmprint identification will be implemented with training, systems acceptance and then brought on-line via a transition from the existing palm-enabled AFIS. Bidder shall also describe how palmprint interfaces and applications will be configured and commissioned.

5. The bidder shall utilize SFPD provided electronic image databases to be supplemented with images scanned in CLIN 0. In addition, the bidder shall utilize an automatic encoding of the existing SFPD latent images to form the baseline Unidentified Latent File (ULF) (NOTE: this would be analogous to lights out latent-palmprint processing). The ULF shall have the

capability to have the automatic encoded latent palmprints be supplemented with manual encodings (see CLIN 5), or electronically converted NEC-based encodings (see CLIN 6).

6. Bidder shall develop an interface with the existing mugshot system so that all booking records are linked to one or more mugshots (photos of face, scars, marks and tattoos).

    6.1. AFIS shall be able to retrieve mugshot images related to a given identification or verification transaction and include in the data payload that is sent back to the requesting workstation or system, including via web services.

    6.2. Bidder shall transfer all source code of mugshot interface to SFPD.

7. Bidder shall develop a 3290 terminal emulation interface with CABLE to retrieve SF# assigned to each individual at booking and insert into the AFIS with the corresponding record(s).

    7.1. SFPD will facilitate bidder access to IT specialists at SFGOV that manage CABLE to enable the building of the interface.

    7.2. Bidder shall transfer all source code of 3290 interface to SFPD upon AFIS system acceptance

    7.3. Interface shall leverage an 'auto fill in' and 'screen-scrape approach' to retrieving SF# assigned by CABLE to each booking record.

8. Bidder shall describe and propose AFIS via CLIN 1, if applicable.

4.3.1.1 PALMPRINT FUNCTIONALITY

9. The required palmprint functionality / system constitutes the electronically and manually converted palmprint, the converted latent files for lights out processing, the hardware required for processing these files and the software and workflow to perform the searching of these files. The capabilities of the palmprint functionality / system shall be based upon commercial-off-the-shelf (COTS) systems. That is, each bidder shall be able to meet the mandatory General and Specific requirements with existing features and functions of bidder's COTS AFIS or palmprint system.

10. Bidder shall also indicate any and all non-mandatory (optional) requirements that bidder shall ship with bidder's COTS palmprint functionality (CLIN 2). The intent of this is to achieve very early deliverable of the palmprint functionality that meets the basic needs of SFPD including forward search for latents utilizing lights out latent searching.

11. CLIN 11 through 14 enables each bidder to bundle and propose additional non-mandatory requirements as customizations, modifications or supplied by a third party (see Appendix D).

4.3.1.2 ARCHITECTURE

12. Bidder shall describe how their COTS product can be implemented into an enterprise SOA / ESB architecture leveraging Web 2.0 compliant web services.

13. Bidder shall describe bidder's COTS palmprint functionality / system architecture and how workflows and business rules are implemented in bidder's palmprint functionality / system.

14. Bidder shall describe bidder's palmprint functionality / system workflow and rules engine and whether a proprietary or 3rd party (brand name) workflow engine is utilized. Bidder shall also describe if bidder's palmprint functionality / system workflows are static, dynamic and/or configurable by SFPD, and if so the level of corresponding difficulty.

15. For ten print processing, the bidder shall describe which identification (1:n and x:n) technique(s) shall be delivered in bidder's COTS palmprint functionality / system. Examples of techniques include filtering using a biometric image-based index, 100% database penetration, fusing search with any corresponding fingerprint data, etc.

  15.1.   Bidder shall not use any alphanumeric text (i.e. biographic or demographic information about the individual) to perform identifications.

4.3.1.3 ALGORITHM AND SYSTEM PERFORMANCE

4.3.1.3.1 ACCURACY

16. Bidder shall describe how SFPD can operate bidder's COTS palmprint functionality / system at a target operational accuracy level of Equal Error Rate = 1×10^{-8} (0.000001%).

17. Bidder shall provide copies of ALL accuracy results of testing conducted by the National Institute of Standards and Technology (NIST) or another independent 3rd party, including all tables, charts and graphs provided to bidder by NIST or 3rd party.

4.3.1.3.2 SPEED

18. Bidder shall propose a system speed for the palmprint functionality / system for all simultaneous transactions below based on metrics provided in Appendix B:

  18.1.   Number of palmprint transactions per minute

  18.2.   Number of latent palmprint transactions per minute

19. Bidder shall describe to SFPD how bidder, or a cited 3rd party, has measured algorithm and system speeds.

20. Bidder shall explain how SFPD can increase system speed in the future (e.g. by adding additional hardware, registering fewer records per server / blade, software/algorithm upgrades, etc.).

4.3.1.4 LATENT CAPABILITY

21. SFPD requires that all latent prints be processed as quickly as possible and therefore requires bidder to implement lights out latent processing for all latents.

  21.1.   Bidder shall implement lights out processing for the initial encoding and searching of the Unsolved Latent File (ULF).

    21.1.1. Bidder shall propose an encoding and searching schedule of latent processing of the ULF that will not slow down the palmprint functionality / system or overwhelm the latent examiners such that the processing of new daily latent cases is not impacted.

21.2.   Bidder should review CLIN 5 for the manual encoding and searching of the ULF and CLIN 6 for the electronic conversion of the ULF from the NEC format including subsequent searching.

22. Bidder shall enable the subsequent manual encoding (re-encoding) of all latents on a priority basis based on crime type, urgency or a specific need.

23. Latents will be searched against the palm print data producing a list of the top 10 candidates in highest score priority at a rate specified by SFPD and configurable within the solution.

24. Bidder shall include a discussion of any expected benefit of incorporating reverse searching capability (palmprint data against ULF) and all impacts upon system performance.

24.1.   Bidder shall explain any resulting increase in identification rates and the rationale for this belief (including any data supporting this).

4.3.2   SYSTEM FEATURES AND FUNCTIONS

12. See **System Features and Functions** under **General Requirements**.

13. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 2" for <u>mandatory</u> requirements.

14. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 2" for <u>desired</u> requirements.

15. Bidder shall provide palmprint functionality / system than supports mixed-resolution operations (both 500ppi and 1000ppi).

16. Bidder shall only implement systems that store the resultant digitized images and alphanumeric text in an ANSI/NIST and/or FBI compliant file format. Bidder shall specify which version of the ANSI/NIST/FBI standard will be used to store all data, for example:

16.1.   ANSI/NIST-ITL 1-2007[13]

16.2.   ANSI/NIST-ITL 2-2008 (XML)[14]

16.3.   FBI Electronic Fingerprint Transmission Specification (EFTS) 7.1[15]

16.4.   FBI Electronic Biometric Transmission Specification (EBTS) 8.x[16]

16.5.   FBI EBTS XML Information Exchange Packet 8.x[17]

17. Bidder shall provide palmprint functionality / system that supports and interfaces with Oracle or SQL persistent storage database delivered under CLIN 4. All AFIS records must be stored in this database.

17.1.   Proprietary database(s) can only exist inside palmprint functionality / system for the purposes of searching or matching palmprints and for fail-over and redundancy.

18. Bidder shall enable system to support required workflow for SFPD operations, including criminal palmprint and latent-palmprint identification and verification processes

---

[13] http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

[14] http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf

[15] http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[16] http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

[17] http://www.fbibiospecs.org/fbibiometric/docs/EBTS-8001-XML_Draft1.zip

18.1.   Bidder shall provide web service that supports all of these matching functions. Bidder shall describe functionality delivered in bidder's COTS palmprint functionality / system web services.

19. Bidder shall deliver the following minimum functionality in the COTS palmprint functionality / system

19.1.   Latent searching selectable as manual or lights out processing (ULF search against palmprint database)

19.2.   palmprint search against ULF database

19.3.   Latent search against unsolved latent (ULF)

19.4.   Palmprint identification and verification functionality

19.5.   Best quality composite tenprint record per SF# as primary record plus multiple incident records including the five (5) most recent bookings and configurable within the solution.

4.3.3   STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

4.3.4   SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

4.3.4.1 DATA MIGRATION

2. Bidder shall migrate palmprint and latent data to the new AFIS.

2.1. Bidder shall auto-encode all SFPD latent images for lights out searching.

2.2. Bidder shall assume all digital images are 500ppi and in FBI/ANSI/NIST file format

3. SFPD will also request a complete set (copy) of image files transmitted by SFPD to CalDOJ in the past to be leveraged during the bidder's populating of the AFIS with existing records.

3.1. Some of CalDOJ-provided records may not be on file at SFPD due to errors and omissions…however it is more likely that all DOJ-provided files will be a subset of the record set currently managed by SFPD.

3.2. The records provided by CalDOJ may include updated fingerprint images (one or all) for the same subject/person that were captured by another agency in the state of California as an update to the record. If these prints are of a higher quality than those on file at SFPD for the same individual, the prints from CalDOJ shall be used.

3.3. Bidder will work with CalDOJ to ensure data is in a format acceptable for use by bidder's palmprint functionality / system

4. SFPD anticipates a complete card conversion at 1000ppi as stipulated in CLIN 0 will be accomplished. The majority of these records have already been scanned at 500ppi previously and registered in the existing palmprint-enabled AFIS.

4.1. The bidder shall import all newly converted cards and extract fingerprint minutiae data at 1000ppi. Any existing corresponding records at 500ppi will be updated with 1000ppi data.

5. Bidder shall ensure that for all data that is migrated, bidder shall maintain complete data integrity and shall ensure that all privacy act requirements are met.

   5.1. For example, no data shall be lost, all data shall be converted properly, the pedigree of the data shall be tracked, original data shall not be altered and no data shall be mixed up or altered.

   5.2. To achieve this, the bidder must submit a Data Conversion and Migration Plan that addresses all of these issues for each type of data and demonstrates that the vendor will convert data properly.

6. Prior to migrating any data, SFPD will require that the bidder convert a set of sample data (records) for each file type that will be migrated.

   6.1. 20 complete files (for each file type) shall be selected by the SFPD and provided to bidder. Bidder shall convert/migrate these 20 files to the new palmprint functionality / system in accordance with the requirements specified.

   6.2. The converted/migrated files will be tested/evaluated by SFPD. If SFPD determines the conversion/migration to be acceptable, an approval document to that effect will be provided to the bidder prior to full data conversion/migration. Upon receipt of this document signed by a proper SFPD authority, bidder shall then perform the full migration/conversion of this particular file type.

4.3.4.2 DATA CLEANSING

7. Bidder shall perform a cleansing of all records in the database to 1) detect all duplicates and aliases; and 2) ensure the highest quality palmprints are committed as a part of the primary/master record for each individual for future identification and verification purposes.

4.3.5   SYSTEM OPERATION

1. See **System Operation** under **General Requirements**.

4.3.6   SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.

2. Prior to system acceptance, the palmprint and latent accuracy requirements shall be tested to verify that the operational system achieves the same or better accuracies than what has been achieved by relevant NIST, FBI and/or other 3rd party testing.

   2.1. Bidder shall recommend and describe a set of test protocols / test plan to satisfy this requirement. SFPD reserves the right to review and approve all proposed test protocols and test plans.

   2.2. SFPD reserves the right to perform additional tests to verify that performance meets or exceeds the accuracies achieved by relevant NIST, FBI or other 3rd party testing.

2.3. After system acceptance, accuracy tests will continue to run on a regular basis to reconfirm system performance and detect any degradation.

3. The palmprint response time requirements (palmprint functionality / system speed) shall be verified after the initial palmprint records have been loaded to that system and cleansed, and prior to system acceptance.

    3.1. A test group shall include a sample of transactions typical to SFPD operations including a statistically significant number of poor quality prints (approximately 3-5%). The bidder and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

    3.2. The test will be deemed successful if the results meet or exceed bidder's COTS palmprint functionality / system response times proposed by bidder.

    3.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

4. The latent response time requirements shall be tested on the COTS palmprint functionality / system after the initial ULF records have been loaded to that system, and prior to system acceptance.

    4.1. A test group will consist of varying image quality and size and shall include a sample of transactions typical to SFPD operations including cases with multiple lifts. The bidder and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

    4.2. The test will be deemed successful if the results meet or exceed bidder's COTS palmprint functionality / system response times proposed by bidder.

    4.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

4.3.6.1 DATA MIGRATION

5. Bidder shall propose a set of system acceptance validations/tests that shall demonstrate the bidder has complied with the Data Conversion and Migration Plan. This set of system acceptance validations/tests, along with the Data Conversion and Migration Plan, must be approved by SFPD before any data migration occurs.

6. During/following conversion completion the vendor/SFPD shall perform the acceptance tests in the Data Conversion and Migration Plan. SFPD will review the acceptance plan results and provide an acceptance or rejection letter signed by the proper SFPD authority to the vendor. Only if the vendor receives the acceptance letter will the conversion be considered complete and accepted.

4.3.7 TRAINING

1. See **Training** under **General Requirements**.

2. The bidder shall train SFPD staff/trainers on all workstation activities, including, but not limited to:

    2.1. palmprint processing

2.2. Latent palmprint processing

2.3. Image acquisition

2.4. Report requests

2.5. Record lookups

2.6. Updating and inserting target records

2.7. System / database administration, configuration, tuning and optimization

4.3.7.1 LATENT PRINT TRAINING

3. Training shall include, but not be limited to;

    3.1. Latent fingerprint entry (use of camera, lighting techniques, use of scanner, calibration tools, search set-up, use of filters, use of printers, use of clarification tools, encoding of minutiae, marking of other print characteristics used by bidder);

    3.2. Latent evaluation;

    3.3. Latent verification;

    3.4. ULF function;

    3.5. Interoperability of entry and evaluation with CalDOJ State

    3.6. Interoperability of entry and evaluation with the FBI/IAFIS including the Universal Latent Workstation (ULW) application

    3.7. Latent image exporting and importing

4.3.7.2 PALMPRINT TRAINING

4. Training shall include, but not be limited to:

    4.1. ABIS Workstation functions,

    4.2. Image acquisition and manipulation,

    4.3. image encoding,

    4.4. image manipulation,

    4.5. data entry,

    4.6. workflow,

    4.7. validation,

    4.8. verification,

    4.9. minutiae placement,

    4.10.   quality control,

    4.11.   diagnostic routines,

    4.12.   backup and recovery functions

4.3.8   SUPPORT AND MAINTENANCE

1. See Support and Maintenance under General Requirements.

4.4   CLIN 3 – FIXED POST ID

4.4.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**

2. SFPD FSD carries out internal mission requirements revolving around solving crimes and identifying individuals. However, SFPD FSD has also committed to offer high quality identity-centric applications and services to authorized stakeholders within the agency and throughout SFGOV. By delivering these applications and services effectively, the information that is gathered, analyzed and cleansed by FSD can become much more powerful to help strengthen the public safety of the citizens of San Francisco and surrounding communities.

3. It is common for SFPD personnel and authorized stakeholder staff to require a positive identification of an individual (suspect, person of interest, person on trial, criminal, parolee, person on probation, etc.) and to be aware of previous criminality prior to initiating (or granting) a set of processes, procedures (or privileges), or during the middle of executing (e.g. verifying) a set of processes, procedures (or privileges); potentially in order to comply with SFGOV, State or Federal laws, policies and/or regulations…or to simply ensure the person is who he or she claims they are.

4. This CLIN focuses on delivering authorized internal and external stakeholders a rapid identification capability using plain impression (flat) fingerprints via a single finger or multi-finger device and a desktop or a laptop computer leveraging web services to interface with the ABIS. Referred to as Fixed Post ID (FPID), this application shall be delivered in a very cost-effective manner with as little negative impact as possible on the computing environment of each user of the application.

5. Although FPID may be installed on laptop computers with wireless connections for some locations, its primary focus is to provide rapid identification capability to permanent facilities with high speed networks throughout SFGOV such as fixed posts, jail facilities, investigator offices, etc. In these scenarios, portability is not a priority; rather ease-of-use and the cost-effectiveness of deployment, support and maintenance must remain the primary foci.

4.4.2   SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**

2. Fingerprint scanners with USB connector to PC USB port
   2.1. Single finger, 2-finger or 4-finger scanner configurations to be deployed on various existing SFPD and stakeholder computers, as well as new desktop/laptop computers
   2.2. Bidder shall accommodate for missing or unusable fingers during capture.
   2.3. Bidder shall provide auto capture for the device and specify what parameters are automatically being checked and adjusted to obtain the best quality image (e.g. gain, contrast, brightness, finger detect, core detect and positioning, ridge presence, surface area of image, etc.).

3. Application Access Controls and Security
   3.1. Bidder shall describe how proposed FPID solution complies with SFPD/SFGOV, CalDOJ/CLETS and FBI CJIS stipulated security and access control standards, requirements, certifications, guidelines and best-practices (e.g. multi-factor authentication of user/operator)
   3.2. Bidder shall discuss their ability to support Citrix for access control to the FPID workstation and application
4. Bidder shall indicate whether the application is a secure graphical user interface built on a thick client, thin client or smart client architecture (e.g. web application)
   4.1. Required workflow and priority support to identify/verify individuals (suspects, persons of interest, known criminals, etc.) against the central ABIS and/or a local watchlist
   4.2. Bidder shall discuss their ability to leverage a COTS application server, workflow server and database server procured by SFPD via CLIN 4 to develop and deliver the application, including if CLIN 4 is procured from a different vendor than for this CLIN (CLIN 3).
5. SFPD recognizes the wide range in the quality of images from affordable fingerprint scanners, including the size of platens and FBI certification status.[18] SFPD also recognizes the difficulty in obtaining high accuracies with plain impression fingerprints without utilizing multiple fingers.
   5.1. Bidder shall describe why a particular vendor and model of fingerprint device is recommended, including benefits, risks and key pros and cons of utilizing said device.
6. SFPD also recognizes the value of fusing facial recognition into the FPID application under the right lighting conditions and if the software application and process remains easy to implement and use.
   6.1. Bidder is encouraged to discuss the option of leveraging the planned FRS (see CLIN 8) and how bidder would fuse the results from the AFIS and FRS to ensure the overall accuracy of the match results remains high.
   6.2. Bidder shall describe why a particular vendor and model of digital camera is recommended, including benefits, risks and key pros and cons of utilizing said device.
   6.3. The FPID application needs to be simplistic in operation and utilize as much information contained in the ABIS and mugshot system as possible to determine identity and provide the following feedback to the operator:
      6.3.1. SF#
      6.3.2. Full Name
      6.3.3. At least one previous arrest photo (e.g. retrieved from the mugshot system)
      6.3.4. List of known crimes the person was arrested (e.g. any available data from livescan/mugshot booking)

---

[18] http://www.fbi.gov/hq/cjisd/iafis/cert.htm - Identification Flats Systems and PIV Single Finger Capture Devices

6.3.5. Any other information available from previous arrests (e.g. any available data from livescan/mugshot booking)

6.3.6. OPTIONAL: Outstanding wants and warrants (likely requires interface to CABLE system…SFPD may opt to activate this option once the new RMS system installation has been completed)

7. Bidder shall provide a minimum operational accuracy level of Equal Error Rate = 1×10^{-5} (0.01%) for the FPID application.

4.4.3   STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements.**
2. The bidder shall only offer fingerprint devices that are FBI certified.
3. FPID hardware device(s) shall comply and/or be certified with the following US and international standards, certifications, best practices, etc. with respect to electrical/electronic devices. Bidder shall submit evidence of certification/compliance.
   3.1. FCC Part 15
   3.2. UL
4. If the FMS (CLIN 8) is to be utilized by the application, the bidder shall specify any and all photo / mugshot standards or best practices that will be used to capture the face.
   4.1. If the FMS (CLIN 8) is to be utilized by the FPID application, the bidder shall only offer multi-megapixel digital cameras that can capture at least ninety (90) pixels between the eyes when the face is approximately five (5) to eight (8) feet from the camera lens

4.4.4   SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.
2. At each designated FPID point-of-use, SFPD will provide one (1) computer or laptop running Windows NT/2000, Windows XP or Windows Vista and at least one (1) USB 1.0 or better port for use with the FPID application (USB 2.0 ports may also be available to enable higher speed communications with the fingerprint device, but this is not guaranteed).
   2.1. Physical desktop space may be limited at certain locations. Devices with smaller footprints and overall physical size are desirable.
   2.2. For locations with fixed PC's, a wired network connection will be available with at least one (1) 10Mbps Ethernet connection or better.
   2.3. For locations with a laptop computer, it is expected that either one (1) 10Mbps Ethernet connection will be utilized, or an 802.11b WiFi connection or better will be available linking back to an access point or router with a permanent 10Mbps Ethernet uplink connection or better.
   2.4. Bidder shall discuss the risks and benefits of using cellular modem cards (2G/3G) inside one or more laptop computers and leveraging a private VPN, Citrix connection or other secure method of remotely accessing the SFPD network to gain access to the ABIS.
3. The bidder shall install the FPID application and required peripherals at the following locations:

Location	Number of FPID Workstations	Address
Central Station (Company A)	1	766 Vallejo Street
Southern Station (Company B)	1	850 Bryant Street
Bayview Station (Company C)	1	201 Williams Street
Mission Station (Company D)	1	630 Valencia St
Northern Station (Company E)	1	1125 Fillmore Street
Park Station (Company F)	**1**	**1899 Waller Street**
Richmond Station (Company G)	1	461 6th Avenue
Ingleside Station (Company H)	1	1 John Young Lane
Taraval Station (Company I)	1	2345 24th Avenue

Tenderloin Station (Company J)	1	301 Eddy Street
SFPD SFO (Airport Bureau)	2	SFO Airport, San Mateo County
Medical Examiner	1	850 Bryant Street
Superior Court	5	Hall of Justice
FSD ID Section	1	Hall of Justice
County Jail #1	1	Hall of Justice, 6th Floor, San Francisco
County Jail #2	1	Hall of Justice, 7th Floor, San Francisco
County Jail #5	2	San Bruno
County Jail #7 (CJ#5 West Building)	1	San Bruno
Ward 7D/7L	1	San Francisco General Hospital
County Jail #8	1	425 7th Street, San Francisco
County Jail #9	1	425 7th Street, near Hall of Justice, San Francisco
San Mateo County Sherriff Location 1	**1**	**Main Jail**
San Mateo County Sherriff Location 2	1	Secondary Jail
Community Justice		575 Polk St, San Francisco

Center

TOTAL   29

4.4.5 SYSTEM OPERATION

1. See **System Operation** under **General Requirements**.
2. At a minimum, bidder shall provide two (2) roaming support persons and two (2) vehicles for the first five (5) days of operations.
   2.1. Roaming support persons will move throughout the San Francisco area to each location where systems are installed on a standard routing schedule, breaking off the schedule only if a call for support arises to drive directly to the location where the support call came in from.
   2.2. One roaming support person will work a ten (10) hour shift from 0800 to 1800.
   2.3. The second roaming individual will operate a ten (10) hour shift from 1800 overnight to 0400.
   2.4. Either support person should be on-call from 0400 to 0800 in case a support request comes in.

4.4.6 SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.
2. Bidder shall demonstrate secure logon to the application as an administrator
3. Bidder shall demonstrate all administrator settings
4. Bidder shall demonstrate logoff the application
5. Bidder shall demonstrate secure logon to the application as a user
6. Bidder shall demonstrate all user-adjustable settings
7. Bidder shall demonstrate the capture of fingerprints (and photo) from an individual (test record)
8. Bidder shall demonstrate the launching of a lights-out search (fingerprint or fingerprint + face)
9. Bidder shall demonstrate the displaying of all available results to the screen, to include:
   9.1. SF#
   9.2. Full Name
   9.3. At least one previous arrest photo (e.g. from the mugshot system)
   9.4. List of known crimes the person was arrested (e.g. any available data from livescan/mugshot booking)
   9.5. Any other information available from previous arrests (e.g. any available data from livescan/mugshot booking)
   9.6. OPTIONAL: Outstanding wants and warrants (likely requires interface to CABLE system)

10. Bidder shall demonstrate the entering of a person's name
11. Bidder shall demonstrate the launching of a filtered search based on person's claimed name
12. See Number 8
13. Bidder shall demonstrate the entering of a person's SF#
14. Bidder shall demonstrate the launching of a filtered search based on SF#
15. See Number 8
16. Bidder shall logoff the application.

4.4.7 TRAINING

1. See **Training** under **General Requirements**.
2. Bidder shall train students on how to capture plain impression fingerprints properly, including
   2.1. positioning of the finger
   2.2. amount of pressure and how to detect under and over pressure
   2.3. how to deal with dry or overly moist fingers
   2.4. how to deal with missing or overly damaged fingers
   2.5. how to deal with other exceptions (e.g. tattoos on finger surface, etc.)
   2.6. what a good fingerprint looks like
   2.7. how and when to override automatic image capture and quality checks for "best effort" searching
3. Bidder shall train students on how to routinely calibrate, clean and maintain the fingerprint device
4. Bidder shall train students on how to deal with and overcome USB communications errors
5. Bidder shall train students on how to capture photographs properly for purposes of searching FRS, if applicable to bidder's proposal, including
   5.1. positioning of the face
   5.2. lighting issues and how to overcome them
   5.3. how to deal with glasses
   5.4. how to deal with other exceptions (e.g. tattoos on face, etc.)
   5.5. what a good photo of the face looks like
   5.6. how and when to override automatic image capture and quality checks for "best effort" searching
6. Bidder shall train students on how to routinely clean and maintain digital camera (e.g. lens), if applicable to bidder's proposal
7. Bidder shall train students on how to deal with and overcome USB communications errors with digital camera, if applicable to bidder's proposal

4.4.8 SUPPORT AND MAINTENANCE

4. See **Support and Maintenance** under **General Requirements**.
5. Bidder shall provide a brief description (with options) of the hardware warranty for the fingerprint devices.

6. Bidder shall provide a brief description (with options) of the hardware warranty for the digital cameras / webcams (if applicable).

4.5   CLIN 4 – APPLICATION, WORKFLOW AND DATABASE ENGINES

4.5.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**
2. SFPD FSD is committed to moving to a Services Oriented Architecture (SOA) and Enterprise Service Bus (ESB) leveraging web services in compliance with the SFGOV JUSTIS initiative and for many other beneficial reasons discussed in Section 1 of this document.
3. Therefore, it has been determined that the ABIS procured under this solicitation include the commercial off the shelf (COTS) framework required to abstract all applications, interfaces, workflow (business process, rules, orchestration, etc.) and the primary persistent database.
4. SFPD FSD understands that not all applications, interfaces and workflows implemented as a part of the new ABIS will be abstracted immediately…and that applications and interfaces may need to be re-built or re-engineered in the future over time. However all bidders shall provide the necessary, capable web services so that, at a minimum, the corresponding proposed CLIN can be treated as a separable 'engine' by the enterprise to satisfy a commitment to extensibility without dependence on a single manufacturer or vendor.
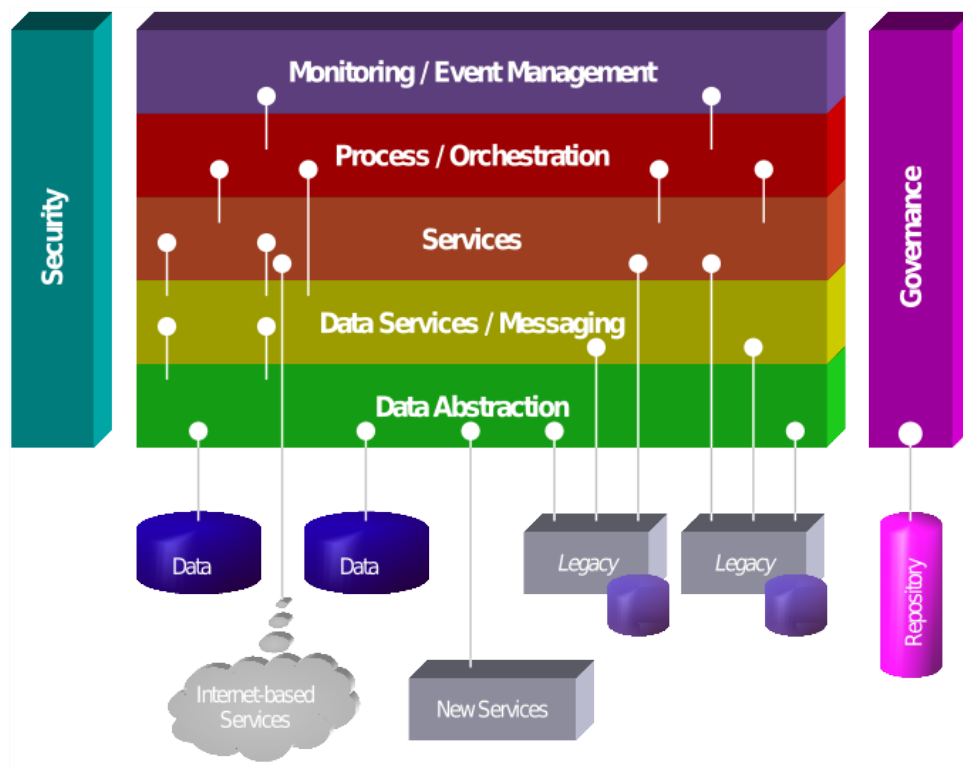
Figure 4 - Notional diagram of Services Oriented Architecture (SOA) principles.

5. To be clear, SFPD and SFGOV have been, and will continue to, develop, acquire and/or contract the expertise to build-out applications and interfaces, manage and modify heavy-volume workflows as well as sophisticated databases. Therefore, regardless of the underlying architecture of each proposed CLIN solution, the core identity services (or engines) delivered in each CLIN shall be addressable via web services.

6. This CLIN is to deliver the ABIS application/interface server, ABIS workflow server and ABIS database server.

4.5.1.1 APPLICATION ENGINE

7. For the purposes of this procurement, the Application Engine is one or more servers (linked as an array) where the COTS web application framework resides to enable the building-out and operation of thin-client and smart-client (e.g. web based) applications and interfaces.

8. SFPD envisions that all thin and smart client applications will be hosted on the Application Engine. Thick client applications that reside on local computers will leverage interfaces and automated routines written via the Application Engine and Workflow Engine to transfer data upstream to the server environment and to receive confirmations and results back from the server environment.

9. SFPD envisions that a brand-name application framework (software) will be implemented.

4.5.1.2 WORKFLOW ENGINE

10. For the purposes of this procurement, the Workflow Engine is one or more servers (linked as an array) where the COTS orchestration software/framework/services reside to enable automated business logic/rules to takes place to support applications and interfaces, as well as the coordination of the exchange of information through web service interactions. It is also envisioned that the Workflow Engine will also manage all transaction-based communications with the Database Engine.

11. SFPD desires that a commercial grade workflow engine (software) will be implemented.

4.5.1.3 DATABASE ENGINE

12. For the purposes of this procurement, the Database Engine is one or more servers (linked as an array) where the COTS database software/framework resides to create a common repository and persistent store of all ABIS data, information, settings, configurations, events, archives, logs, etc.

13. The Database Engine is managed by the Workflow Engine, which ensures that only the right data is modified/read at the right time by the right application.

14. The Database Engine will also allow direct connections from various identity engines (such as the AFIS and FRS) to offer table services to these engines to enable their proper operation, backup and recovery.

15. SFPD envisions that either Microsoft SQL or Oracle database will be implemented to match the skill sets of SFGOV support staff.

4.5.2   SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.

2. **Services Oriented Architecture**

   2.1. Bidder shall describe how the products support an enterprise SOA.

   2.2. Bidder shall diagram SOA reference architecture and cross reference product names, descriptions, high-level features and roles.

   2.3. For the products listed in bidder's SOA reference architecture, bidder shall identify the COTS and custom development tools used for each product and how these tools interoperate - e.g. how does a BPM tool interoperate with the ESB from a developer's perspective?

   2.4. Bidder shall describe how bidder's product fits with other related architectures and products such as model driven architecture, event driven architecture, complex event processing, business rule process and business process management? Bidder shall list any formal products that support these concepts.

   2.5. Bidder shall describe bidder's products' support for XML (design, authoring, etc).

   2.6. Bidder shall describe how best to integrate with the existing systems described in section 2 of this document.

2.7. Bidders shall describe how bidder will create web services to expose functionality to the existing systems described in section 2 of this document.

2.8. Bidder shall describe how bidder's product will orchestrate available web services in an end-to-end business process and what products are needed.

2.9. Bidder shall describe the security architecture of bidder's solution.

2.10. Bidder shall describe bidder's approach to create Rich Internet Applications interfaces as composite applications.

2.11. Bidder shall describe bidder's deployment, monitoring and management platform for SOA that enables composite applications to be developed, deployed and managed as distributed, standards-based services.

2.12. Bidder shall describe any and all support the Java Specification Request (JSR) 208 - the Java Business Integration (JBI) specification - and what the standards role in the product architecture is.

2.13. Bidder shall describe the integration development lifecycle, specifically how bidder's transition integration project between design time and run-time.

2.14. Bidder shall describe if the bidder's solution requires an application server and if so list the COTS application servers supported.

2.15. Bidder shall describe how bidder's products support XML, XSD, XSLT, XPath, and WSDL. Are these standards used for internal representation of the tools models and data?

2.16. Bidder shall list standard formats that can be imported and exported from bidder's modeling tools.

2.17. Bidder shall describe how bidder supports data cross-referencing and caching?

2.18. Bidder shall describe how bidder integrates with ETL and master data management tools.

2.19. Bidder shall describe bidder's development lifecycle for the development tools in bidder's product stack including the high-level steps and tools that support design, development, testing, deployment and asset management.

2.20. Bidder shall describe how bidder's services are deployed, monitored and maintained. Also how source control systems are supported.

3. Bidder shall propose a database system that can manage up to 1 million biometric-based criminal/person records and the transaction rates described in Appendix B (AFIS, Fixed Post ID, Mobile ID, etc.), including the following at a minimum for each person-record:

3.1. Basic demographic and biographic data (equivalent to the data captured during an arrest/booking).

3.2. Facial Image data including both images and templates (including multi-megapixel images of front, left side and right side of face as well as full frontal photo of entire person/body including face).

3.3. Scars, marks and tattoo data (including up to 20 multi-megapixel images per person).

3.4. Fingerprint data including images and templates (including all 10 rolled fingerprints and templates, all multi-finger slap images and all 10 segmented slap images).

3.5. Palm print data including images and templates (including upper palm, lower palm, thenar, hypothenar and writer's palm).

4. Bidder shall describe the amount of hardware and software required for data storage and database capacity for each 0.5 Terabyte (TB) increment.

5. **Enterprise Service Bus and Messaging**

   5.1. Bidder shall describe how bidder's product supports large data volumes including large message sizes and high arrival rates (include limitations).

   5.2. Bidder shall describe bidder's support for JMS (including version) and any proprietary extensions.

   5.3. Bidder shall describe the message patterns and protocols supported - e.g. publish/subscribe, synchronous/asynchronous, push/pull/pool, topics/queues.

   5.4. Bidder shall describe if bidder offers client protocols for Java, .NET and C ++/C#

   5.5. Bidder shall indicate if bidder's product supports messaging infrastructure COBOL data structures (e.g. copybooks).

   5.6. Bidder shall describe what other transports other than HTTP can be configured in bidder's product to use for SOAP messages.

   5.7. Bidder shall describe bidder's scalability and load balancing solutions.

   5.8. Bidder shall describe supported High Availability (HA) scenarios and list required products (including third party). Does it support automated fail over?

   5.9. Bidder shall describe if bidder's product guarantee once and only once message delivery in the original message sequence.

      5.9.1. Bidder shall list any scenarios where this is not support – (e.g. load balancing).

   5.10.   Bidder shall describe message persistence scenarios.

   5.11.   Bidder shall describe support for message delivery notification, exception handling, logging, dead letter queues, security (access control architecture), message encryption

   5.12.   Bidder shall describe support for FTP, file and database connectivity including adapter scenarios.

   5.13.   Bidder shall specify the downtime requirement for configuration changes and upgrades.

6. **Metadata Management**

   6.1. Bidder shall describe if bidder's product includes a metadata repository

      6.1.1. Is there a centralized, single product repository across your SOA product line?

   6.2. Bidder shall indicate if bidder's metadata repository can be geographically distributed and federated.

      6.2.1. How does the product support data distribution and reconciliation?

   6.3. Bidder shall describe the development lifecycle and governance support for metadata and services.

   6.4. Bidder shall list the products that use the metadata repository including relevant third-party tools.

6.5. Bidder shall describe version control and impact analysis in the tools.

6.6. Bidder shall indicate how repository data is viewed and queried.

6.7. Bidder shall indicate whether bidder's product provides graphical representations of metadata and service linkages.

6.8. Bidder shall describe any and all standards support including UDDI

6.9. Bidder shall specify if bidder supports the following data formats (your list e.g. EDI, X12, HL7, etc.)?

7. Process Orchestration

7.1. Bidder shall specify whether bidder's product in this area is considered a BPM offering.

7.2. Bidder shall explain how business models are migrated to execution models.

7.3. Bidder shall describe the different reporting types, metrics, auditing, etc., available in the tool.

7.4. Bidder shall describe bidder's products HA and scalability features if different from above.

7.5. Bidder shall highlight any and all debugging features.

7.6. Bidder shall indicate whether bidder's product supports Key Process Indicators.

7.7. Bidder shall describe bidder's security model and standards support in this area.

7.8. Bidder shall describe the development lifecycle and support for version control and change management.

7.9. Bidder shall indicate whether work items can be load balanced and auto-routed across both roles and specific users based on skill set or other parameters.

7.10.   Bidder shall indicate whether the product includes a form design module to speed creation of actions.

7.11.   Bidder shall explain how bidder's product supports business partners, customers, suppliers and other outside entities.

7.12.   Bidder shall explain how bidder's product delivers information to users and applications.

7.13.   Bidder shall indicate whether bidder's product includes BAM and predictive capability.

7.14.   Bidder shall describe your support for CEP, rules and task priorities.

7.15.   Bidder shall describe the modeling tool and diagramming processes including the role perspective (e.g. business user versus developer).

7.16.   Bidder shall describe how bidder's tool supports manual intervention and rework of in-flight tasks.

7.17.   Bidder shall describe how bidder manages and reuses processes and rules.

7.18.   Bidder shall describe bidder's simulation capabilities.

7.19.   Bidder shall describe your infrastructure requirements.

8. Monitoring & Management

8.1. Bidder shall describe the architecture and components of bidder's management and monitoring tool?

8.2. Bidder shall indicate whether bidder's product supports component availability, logging, tracking of events, problem determination, and performance analysis and what tools are required.

8.3. Bidder shall describe monitoring integration with Enterprise Management tools such as HP OpenView.

8.4. Bidder shall describe integration with problem management tools.

9. **Database Engine**

9.1. Bidder shall provide the latest general release of Microsoft SQL or Oracle database.

4.5.3　STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

4.5.4　SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

4.5.5　SYSTEM OPERATION

1. See **System Operation** under **General Requirements**.

4.5.6　SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.

2. Bidder shall demonstrate the building and execution of a sample web application on the Application Engine that utilizes the Workflow Engine and Database Engine

   2.1. SFPD prefers if this sample web application is administrative in nature, such as a digital dashboard application, to serve as a basis to develop the ABIS Administration Software (Dashboard) going forward.

   2.2. Bidder shall provide a features and functions list for this sample application

3. Bidder shall demonstrate any other administrative interfaces or applications that will be provided with the Application Engine, Workflow Engine and Database Engine listed and described in bidder's proposal

   3.1. Bidder shall demonstrate the graphical user interface(s) for the Workflow Engine

   3.2. Bidder shall demonstrate the building of several sample workflows related to identity management and biometrics

4. Bidder shall demonstrate a full backup and restore of the Database Engine

5. Bidder shall demonstrate fail-over and redundancy capabilities of the Application Engine, Workflow Engine and Database Engine

6. Bidder shall demonstrate that the Application Engine, Workflow Engine and Database Engine are all installed per manufacturers' recommendations including naming conventions, schema structures, table management, tunings and optimizations, latest updates and service packs, etc.

4.5.7 TRAINING

1. See **Training** under **General Requirements**.
2. Bidder shall provide a full classroom-based training course through the 'intermediate level' for up to three (3) SFPD/SFGOV students for all COTS software installed, either directly or via a 3rd party, except for the Database Engine

4.5.8 SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.

4.6 CLIN 5 – LATENT ENCODING

4.6.1 SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**
2. After the basic AFIS and palmprint functionality / system capabilities have been accepted, the SFPD will determine how and when it wants to proceed with the other latent (palm and tenprint) encodings. The options currently under consideration by SFPD include:
   2.1. SFPD latent staff will manually re-encode lights out encoded latents over time (no additional CLINS)
   2.2. Initial manual encodings of the ULF leveraging bidder-provided staff (CLIN 5)
   2.3. Existing NEC formatted manual latent encodings are electronically (automatically) converted (CLIN 6) to a format usable (searchable) by the new AFIS and palmprint system.
   2.4. If bidder has other suggestions, bidder should propose them and the rationale for it

4.6.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.
2. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 5" for <u>mandatory</u> requirements.
3. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 5" for <u>desired </u>requirements.

4.6.3 STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

4.6.4 SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.
2. Bidder shall create new latent database with manual extraction / encoding procedures.
3. Bidder shall provide all necessary latent examiners for encoding
   3.1. Examiners to be managed by a SFPD approved latent examiner.

4. SFPD shall approve bidder's manual latent encoding process.
   4.1. Initial lights-out latent encodings delivered in CLIN 1 and CLIN 2 can be used as a baseline in this CLIN

4.6.5   SYSTEM OPERATION
1. See **System Operation** under **General Requirements**.

4.6.6   SYSTEM ACCEPTANCE
1. See **System Acceptance** under **General Requirements**.

4.6.7   TRAINING
1. See **Training** under **General Requirements**.

4.6.8   SUPPORT AND MAINTENANCE
1. See **Support and Maintenance** under **General Requirements**.

4.7   CLIN 6 – LATENT ENCODING, ELECTRONIC CONVERSION

4.7.1   SCOPE OF IMPLEMENTATION AND OPERATION
1. See **Scope of Implementation and Operation** under **General Requirements.**
2. After the basic AFIS and palmprint functionality / system capabilities have been accepted, the SFPD will determine how and when it wants to proceed with the other latent (palm and tenprint) encodings. The options currently under consideration by SFPD include:
   2.1. SFPD latent staff will manually re-encode lights out encoded latents over time (no additional CLINS)
   2.2. Initial manual encodings of the ULF are completed by bidder-provided staff (CLIN 5)
   2.3. Existing NEC formatted manual latent encodings are electronically (automatically) converted to a format usable (searchable) by the new AFIS and palmprint system (CLIN 6).
   2.4. If bidder has other suggestions, bidder should propose them and the rationale for it.
3. For CLIN 6, bidder shall provide the automated conversion of the existing NEC encoded latent files to the new AFIS and palm functionality/system format or another format usable (searchable) by the new AFIS and palm functionality/system (such as Universal Latent Workstation format for example).

4.7.2   SYSTEM FEATURES AND FUNCTIONS
1. See **System Features and Functions** under **General Requirements**.
2. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 6" for <u>mandatory</u> requirements.
3. Please see SFPD ABIS TRFP-Requirements.doc "CLIN 6" for <u>desired </u>requirements.

4.7.3   STANDARDS COMPLIANCE

1.   See **Standards Compliance** under **General Requirements**.

4.7.4   SYSTEM INSTALLATION

1.   See **System Installation** under **General Requirements**.
2.   NEC encoded latents will be provided to the bidder by SFPD

4.7.5   SYSTEM OPERATION

1.   See **System Operation** under **General Requirements**.

4.7.6   SYSTEM ACCEPTANCE

1.   See **System Acceptance** under **General Requirements**.

4.7.7   TRAINING

1.   See **Training** under **General Requirements**.

4.7.8   SUPPORT AND MAINTENANCE

1.   See **Support and Maintenance** under **General Requirements**.

4.8   CLIN 7 - LIVESCAN STATIONS

4.8.1   SCOPE OF IMPLEMENTATION AND OPERATION

1.   See **Scope of Implementation and Operation** under **General Requirements.**
2.   SFPD operates a number of existing livescan workstations that support 10-print and/or palmprint capabilities.
3.   SFPD requires a minimum of three (3) and a maximum of seven (7) new/replacement livescan systems that optimize automated functions while still enabling manual overrides on a case-by-case basis SFPD envisions that other biometric data may also be collected in the future on these same replacement livescan systems, including photographs (face - mugshots, scars, marks and tattoo images), iris images, etc. Bidder shall describe what capture modules can be added on to livescan unit immediately or in the future via a field upgrade.
   3.1. Bidder shall describe whether data capture of these other biometric data will be available immediately via the proposed CLIN or through a future modular add-on to the livescan unit
   3.2. Livescan shall enable administrator to turn on and off any additional biometric capture modules (e.g. mugshot, iris, etc.) as needed or required

4.8.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.
2. Construction
   2.1. Livescan will be delivered by bidder in a rugged housing (e.g. casing, cabinet, etc.) optimized for durability, usability and the smallest footprint possible
   2.2. Bidder shall describe the pros and cons of SFPD implementing cabinet-based systems versus desktop-based systems (e.g. footprint/size, cost, durability, capability, mount-ability, etc.)
3. Application Access Controls and Security
   4.2. Bidder shall describe how livescan system complies with SFPD/SFGOV, CalDOJ and FBI CJIS stipulated security and access control standards, requirements, certifications, guidelines and best-practices (e.g. multi-factor authentication of user/operator)
   4.3. Bidder shall discuss their ability to support Citrix for access control to the FPID workstation and application
4. Data Capture
   4.1. Bidder shall provide livescan system that can capture the following data:
      4.1.1. All fingerprint data, including nail-to-nail rollprints, multi-finger slap prints and fingertips
      4.1.2. All palmprint data including upper palm, lower palm, thenar, hypothenar and writer's palm
      4.1.3. All biographic data related to a criminal arrest in compliance with SFPD, CalDOJ and FBI requirements, guidelines, principles and best-practices
      4.1.4. Multiple digital mugshot images including front, right profile/side and left profile/side facial images
         4.1.4.1.   Must be configurable to turn this feature off
      4.1.5. Multiple scar, mark and tattoo images
         4.1.5.1.   Must be configurable to turn this feature off
      4.1.6. **OPTIONAL:** images of both irises
         4.1.6.1.   Must be configurable to turn this feature off
      4.1.7. **OPTIONAL:** other image data, biometric or photographic (bidder to specify)
         4.1.7.1.   Must be configurable to turn this feature off
   4.2. Livescan system shall capture data in real-time with a preview viewable on the screen as data is being captured
      4.2.1. All image data must be presented on screen in an "up-right" orientation just as the biometric is being captured…fingerprints and palmprints in the vertical…mugshots in landscape orientation.
   4.3. Livescan shall provide multiple methods of capture include keyboard commands, mouse commands and foot-pedal commands.
5. Data Quality Assurance
   5.1. Bidder shall describe all image quality and biographic (alphanumeric) quality assurance routines and algorithms including any and all 3rd party validations and/or certifications.

5.2. Livescan shall measure image quality of each biometric sample in real time such that all proprietary and/or ANSI/NIST NFIQ image scores are presented on-screen immediately after the capture of single biometric sample is complete.

    5.2.1. Proprietary fingerprint image quality should be presented in an equivalent scoring approach as the NIST NFIQ image quality measurement (e.g. scale form 0 to 100, score of 75 is higher quality than score of 65, etc.)

    5.2.2. Other image scoring (e.g. face, iris, etc.) shall use industry standards and/or best-practices

    5.2.3. Administrator shall be able to determine the minimum image quality score acceptable by the system. Bidder shall specify a default setting (or range) as a best-practice.

5.3. Livescan system shall allow manual overrides of any and all image quality assurance routines or algorithms on an exception basis via a privileged operator or administrator

5.4. Livescan will have the ability to mark registration record with unusable or missing fingers, palms and irises (if applicable)

6. Record Formatting

6.1. Bidder shall describe the various file and data format options that will be delivered with this CLIN as a COTS product offering (criminal, civil applicant, registrant, etc.)

    6.1.1. Bidder shall provide details about all SFPD, CalDOJ and FBI record formats that are supported

6.2. Livescan system shall store the image quality score with each corresponding biometric sample

6.3. Livescan shall have the option to segment all multi-finger slap images to create a 20-finger record (ten rollprints and ten segmented slap images)

7. Record Storage

7.1. Livescan shall securely store a local copy of each registration (booking) record for a configurable amount of time as a temporary backup

7.2. Livescan shall not delete any records that were not tracked (recognized) as successfully delivered to ABIS

7.3. Bidder shall describe storage architecture and security of livescan with regards to local data storage (e.g. encryption type and strength, COTS database used, etc.)

8. Record Transmission

8.1. Livescan shall communicate via a hardwired SFPD provided network connection (minimum of 10Mbps Ethernet)

8.2. Bidder shall describe any and all communications security available with livescan to protect data payload as it transits SFPD/SFGOV networks (e.g. encryption type and strength, etc.)

8.3. Bidder shall indicate whether the application is a secure graphical user interface built on a thick client, thin client or smart client architecture (e.g. web application)

8.3.1. Bidder shall provide required workflow and priority support to register individuals (suspects, persons of interest, known criminals, arrestees, etc.) into the central ABIS

8.3.2. Bidder shall describe their ability to interface with existing Identix (L1) store-and-forward servers/systems

8.3.3. Bidder shall discuss their ability to leverage a COTS application/interface server, workflow server and database server procured by SFPD via CLIN 4 to develop and deliver the solution, including if CLIN 4 is procured from a different vendor than for this CLIN (CLIN 3).

     8.3.3.1. More specifically, bidder shall describe their ability to use (or interface with) solution procured in CLIN 4 to perform store-and-forward processes to move data to, and store data in, the AFIS, palm system, mugshot system and FRS leveraging web services.

9. Results of Search

     9.1. Bidder shall describe livescan's ability to retrieve and display the results of the AFIS, palm and/or facial identification and/or verification queries

10. Bidder shall provide copies of ALL results of testing conducted by the National Institute of Standards and Technology (NIST), including all tables, charts and graphs provided to bidder by NIST.

     10.1. Bidder shall organize NIST test results by 1) NIST test type / name and 2) by the bidder's algorithm identifier assigned by NIST and used in the NIST test. Bidder shall include test results from the following NIST tests if bidder participated:

        10.1.1. Slap Fingerprint Segmentation Evaluation (SlapSeg and SlapSegII)

        10.1.2. NFIQ Compliance Testing

     10.2. Bidder shall specify and identify which algorithm(s) used in NIST testing shall be included in bidder's COTS AFIS proposed to be delivered to SFPD.

        10.2.1. If bidder proposes a later and more accurate (better performing) algorithm, bidder shall provide version number in relationship with any applicable NIST results along with any independent 3rd party test results that are available.

4.8.3 STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

2. Bidder (bidder's proposed product) must be certified by CalDOJ as an approved livescan vendor (device).

3. Bidder (bidder's proposed product) must be certified by CalDOJ for the DNA Collection Automation LiveScan program

     3.1. If bidder (or bidder's product) is not certified for the DNA Collection Automation LiveScan program, bidder must demonstrate the application process has begun to become certified for the DNA Collection Automation LiveScan program

4. Livescan device shall comply and/or be certified with the following US and international standards, certifications, best practices, etc. with respect to electrical/electronic devices. Bidder shall submit evidence of certification/compliance.
   4.1. FCC Part 15
   4.2. UL
   4.3. Bidder shall indicate any other similar international compliances and certifications such as CE, Canadian ICES, etc.
5. Bidder shall only implement scanning hardware and software that are listed on the FBI master listing of certified scanning systems/devices.[19] SFPD reserves the right to inspect all hardware and software to ensure model and part numbers match those indicated on letters of certification issued by the FBI.
6. Bidder shall only implement JPEG2000 image compression algorithms that have been certified by the FBI. SFPD reserves the right to request a certified copy of the certification letter from the FBI and require bidder to demonstrate the installed JPEG2000 algorithm matches the algorithm indicated on the certification letter.
7. Bidder shall only implement systems that store the resultant digitized images and alphanumeric text in an ANSI/NIST and/or FBI compliant file format. Bidder shall specify which version of the ANSI/NIST/FBI standard will be used to store all data, for example:
   7.1. ANSI/NIST-ITL 1-2007[20]
   7.2. ANSI/NIST-ITL 2-2008 (XML)[21]
   7.3. FBI Electronic Fingerprint Transmission Specification (EFTS) 7.1[22]
   7.4. FBI Electronic Biometric Transmission Specification (EBTS) 8.x[23]
   7.5. FBI EBTS XML Information Exchange Packet 8.x[24]
8. Bidder shall describe any and all support for the Global Justice XML and NIEM standards.
9. The bidder shall specify any and all alphanumeric (biographic, demographic, etc.) standards and best practices that will be used to capture the alphanumeric data.
10. The bidder shall specify any and all fingerprint and palmprint standards and best practices that will be used to capture the fingerprint and palmprint images.
11. The bidder shall specify any and all photo / mugshot standards and best practices that will be used to capture the face.
    11.1.   The bidder shall only offer multi-megapixel digital cameras that can capture at least ninety (90) pixels between the eyes when the face is approximately five (5) to eight (8) feet from the camera lens

---

[19] http://www.fbi.gov/hq/cjisd/iafis/cert.htm

[20] http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

[21] http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf

[22] http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[23] http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

[24] http://www.fbibiospecs.org/fbibiometric/docs/EBTS-8001-XML_Draft1.zip

12. The bidder shall specify any and all photographic standards and best-practices that will be used to capture the scar, mark and tattoo images

13. The bidder shall specify any and all iris standards and best practices that will be used to capture the iris images.

14. The bidder shall specify any and all other biometric or imaging standards and best-practices that will be used to capture any other biometric or photographic images

4.8.4   SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

4.8.5   SYSTEM OPERATION

1. See **System Operation** under **General Requirements**.

4.8.6   SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.

2. Bidder shall demonstrate multi-factor logon to the livescan system of an administrator and an operator
   2.1. Bidder shall demonstrate the enrollment and administration of system administrators and operators.
   2.2. OPTIONAL: Bidder shall demonstrate the use of Citrix to logon.

3. Bidder shall perform five (5) complete arrest bookings including biographic data, ten-print (rolls and slaps) and palm print (all sections of the palm)

4. Bidder shall demonstrate data is properly formatted per required (cited) standards

5. Bidder shall demonstrate data is securely stored locally for a temporary amount of time until data is transmitted

6. Bidder shall demonstrate the forwarding of all data in the proper format either 1) through the existing store-and-forward servers or 2) utilizing the application/interface, workflow and database engines procured in CLIN 4.

7. OPTIONAL: Bidder shall demonstrate the retrieval of the results of the ABIS search and display results to the screen

8. Bidder shall demonstrate all error messages and error handling in the system, including communications errors

9. Bidder shall demonstrate all event and audit logs in the system, including storage, retrieval and display
   9.1. OPTIONAL: Bidder shall demonstrate the writing of all logs to the database server procured in CLIN 4

4.8.7   TRAINING

1. See **Training** under **General Requirements**.

2. Bidder shall provide expert training on livescan equipment to at least three (3) personnel from SFPD

3. Train the trainer training must also be accomplished with at least one (1) of these same personnel

4.8.8   SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.

4.9   CLIN 8 - FACE RECOGNITION SYSTEM (FRS)

4.9.1   SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**

2. SFPD recognizes that leveraging multiple biometric modalities can significantly increase the chances of concluding a positive identification, gaining investigative intelligence or solving a crime. Furthermore, having the capability to fuse facial matching/identification results with the results provided by fingerprint and/or palmprint matching is very desirable, especially when print quality is less than adequate.

    2.1. For example, CCTV footage and digital photographs are available to SFPD FSD to help identify suspects, victims and missing persons. The quality and amount of this visual information continues to increase as the quality of CCTV and standard digital cameras continue to improve and become more pervasive. Moreover, law enforcement does not always have access to reference fingerprint imagery for specific population groups (e.g. gang members and affiliates, known terrorists, wanted persons, missing persons, witnesses, suspects, etc.).

3. Finally, the accuracy, resilience and flexibility of facial recognition systems (FRS) have greatly improved over the last several years with law enforcement more readily solving cases with the help of such digital facial technology and accompanying tools and best practices.

4. Therefore, SFPD desires a robust FRS to both operate independently as needed or required, as an investigative and identification tool and to deliver the capability to fuse facial matching results with the results provided by the fingerprint and palm print matching systems.

5. Bidder should discuss the various applications relevant to law enforcement where the offered FRS has been used successfully.

4.9.1.1.1 ACCURACY

6. Bidder shall describe how SFPD can operate bidder's COTS FRS at a target operational accuracy level of Equal Error Rate = 1×10^{-2} (1%) or better.

7. Bidder shall provide copies of ALL accuracy results of testing conducted by the National Institute of Standards and Technology (NIST), including all tables, charts and graphs provided to bidder by NIST.

7.1. Bidder shall organize NIST test results by 1) NIST test type / name and 2) by the bidder's algorithm identifier assigned by NIST and used in the NIST test.

8. Bidder shall specify and identify which algorithm(s) used in NIST testing shall be included in bidder's COTS FRS proposed to be delivered to SFPD.

    8.1. If bidder proposes a later and more accurate algorithm, bidder shall provide version number in relationship with any applicable NIST results along with any independent 3rd party test results that are available.

4.9.1.1.2 SPEED

9. Bidder shall propose a system speed for the COTS FRS for all simultaneous transactions below based on metrics provided in Appendix B:

    9.1. Number of booking transactions per minute

    9.2. Number of FPID transactions per minute

    9.3. Number of MID transactions per minute

10. Bidder shall describe to SFPD how bidder, or a cited 3rd party, has measured algorithm and system speeds.

11. Bidder shall explain how SFPD can increase system speed in the future (e.g. by adding additional hardware, registering fewer records per server / blade, software/algorithm upgrades, etc.).

4.9.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.

2. The conversion of the mugshot records from mugshot system forming the searchable FRS database;

3. Bidder shall provide the operational capability for a positive identification (lights out and/or candidate list based) from a facial image:

    3.1. Direct search of the mugshot (FRS) database with a photograph of the suspect, for example from the FPID application (see CLIN 3) or Mobile ID device camera (see CLIN 9), or from a scan of one or more pictures from an investigation;

    3.2. Search of the mugshot (FRS) database with a composite picture;

    3.3. Search of the mugshot (FRS) database with a usable picture from a CCTV/surveillance camera.

4.9.3 STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

2. Bidder shall only implement systems that store the resultant digitized images and alphanumeric text in an ANSI/NIST and/or FBI compliant file format. Bidder shall specify which version of the ANSI/NIST/FBI standard will be used to store all data, for example:

2.1. ANSI/NIST-ITL 1-2007[25]

2.2. ANSI/NIST-ITL 2-2008 (XML)[26]

2.3. FBI Electronic Fingerprint Transmission Specification (EFTS) 7.1[27]

2.4. FBI Electronic Biometric Transmission Specification (EBTS) 8.x[28]

2.5. FBI EBTS XML Information Exchange Packet 8.x[29]

3. Bidder shall describe any and all support for the Global Justice XML and NIEM standards.

4.9.4   SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

4.9.5   SYSTEM OPERATION

1. See **System Operation** under **General Requirements**.

4.9.6   SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.

2. Prior to system acceptance, the FRS accuracy requirements shall be tested to verify that the operational system achieves the same or better accuracies than what has been achieved by relevant NIST and/or other independent and authoritative 3rd party testing.

2.1. Bidder shall recommend and describe a set of test protocols / test plan to satisfy this requirement.   SFPD reserves the right to review and approve all proposed test protocols and test plans.

2.2. SFPD reserves the right to perform additional tests to verify that performance meets or exceeds the accuracies achieved by relevant NIST and/or other independent and authoritative 3rd party testing.

2.3. After system acceptance, accuracy tests will continue to run on a regular basis to reconfirm system performance and detect any degradation.

3. The FRS response time requirements (FRS speed) shall be verified on the FRS after the initial mugshot records have been loaded to that system and cleansed, and prior to system acceptance.

3.1. A test group shall include a sample of transactions typical to SFPD operations including a statistically significant number of poor quality images (approximately 3-5%). The bidder and SFPD shall execute the test, and SFPD shall validate the test results provided by the bidder.

---

[25] http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

[26] http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf

[27] http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[28] http://www.fbibiospecs.org/fbibiometric/documents/EBTS_v8.1_11-24-08.pdf

[29] http://www.fbibiospecs.org/fbibiometric/docs/EBTS-8001-XML_Draft1.zip

3.2. The test will be deemed successful if the results meet or exceed bidder's COTS FRS response times proposed by bidder.

3.3. After system acceptance, response time tests will continue to be executed by SFPD personnel on a weekly basis using a smaller test group.

4.9.7 TRAINING

1. See **Training** under **General Requirements**.

4.9.8 SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.

4.10 CLIN 9 – MOBILE ID PILOT SYSTEM

4.10.1 SCOPE OF IMPLEMENTATION AND OPERATION

1. See **Scope of Implementation and Operation** under **General Requirements.**

2. SFPD FSD carries out internal mission requirements revolving around solving crimes and identifying individuals. However, SFPD FSD has also committed to offer high quality identity-centric applications and services to authorized stakeholders within the agency and throughout SFGOV. By delivering these applications and services effectively, the information that is gathered, analyzed and cleansed by FSD can become much more powerful to help strengthen the public safety of the citizens of San Francisco and surrounding communities.

3. It is common for SFPD personnel and authorized stakeholder staff to require a positive identification of an individual (suspect, person of interest, person on trial, criminal, parolee, person on probation, etc.) and to be aware of previous criminality prior to initiating (or granting) a set of processes, procedures (or privileges), or during the middle of executing (e.g. verifying) a set of processes, procedures (or privileges); potentially in order to comply with SFGOV, State or Federal laws, policies and/or regulations…or to simply ensure the person is who he or she claims they are.

4. More specifically, officers and investigators in the field need to have this functionality delivered in a small, rugged, mobile package that can be carried with them or in their mode of transportation (car, motorcycle, Segway®, ATV, bike, etc.) wherever they go.

5. This CLIN focuses on delivering authorized internal and external stakeholders a rapid identification capability using plain impression (flat) fingerprints (single finger or multi-finger) via an integrated mobile device leveraging a secure communications link and web services to interface with the ABIS. Referred to as Mobile ID (MID), this application shall be delivered in a very cost-effective manner with as little negative impact as possible on the operational environment of each carrier of the device.

6. Each officer in the field is already burdened with many tools of the trade, including electronic devices such as radios, electronic control devices (such as Tasers®), mobile

phones, etc. It is desirable that the MID device is of a small size that fits in the palm of one hand, slides into a shirt-pocket or between the buttons on the shirt (inside the shirt front) or into a pouch or clipped into an eyelet on the officer's belt.

7. Based on extensive stakeholder interviews, the goal of SFPD FSD is to enable 'just enough' identity-centric capability in the field to help make decisions and improve officer safety without overwhelming the officer with too much information, features, functions or capabilities. Many stakeholders desired the following basic functionality:

   7.1. A built-in cellular modem connection for communications (2G/3G)

   7.2. Software that complies with FBI, CalDOJ CJIS and SFGOV/SFPD access control and security rules and regulations

   7.3. Simple 'Red Light' / 'Green Light' response representing criminal history status

      7.3.1. OPTIONAL: Include wants and warrants status in the 'Red Light' / 'Green Light' decision logic

         7.3.1.1.   May require interface to existing or legacy systems such as CABLE/RMS/JMS system…bidder shall discuss this option and indicate level of effort

   7.4. Display of the SF# for the person (received from AFIS/ABIS system)

   7.5. Display of the most grievous crime the individual has been arrested for in the past (type of crime) (received from AFIS/ABIS system)

   7.6. OPTIONAL: Display of whether or not the individual is a sex offender or a juvenile

      7.6.1. May require interface to existing or legacy systems such as CABLE/RMS/JMS system…bidder shall discuss this option and indicate level of effort

   7.7. OPTIONAL: A black and white or color photo of the individual from the most recent booking

      7.7.1. Bidder shall indicate if bidder's MID device's screen remains small enough to make the overall device smaller in size while still possessing the ability to display a reasonable quality black and white or color photo

4.10.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.

2. Bidder shall provide an operational accuracy level of Equal Error Rate = 1×10^{-4} (0.01%) for the MID application.

3. The MID device shall be rugged in construction, durable and resistant to liquids.

4. The MID device shall be easily operated using only one hand (e.g. thumb-driven, quick-launch buttons on side of device, etc.)

5. The MID device shall enable a minimum of 4 hours of continuous use and 10 hours of normal use

   5.1. Bidder shall describe any and all energy saving techniques deployed in the device (e.g. auto standby, auto shutdown, low power mode, etc.)

6. The display of the MID device shall utilize backlighting and other brightening and contrast-enhancing techniques to enable usage both in direct, full sunlight and in the dark.

6.1. The display on the MID device shall be scratch and damage resistant/proof.
7. The MID device shall support cellular (GSM/GPRS, EDGE, W-CDMA), and WiFi (802.11 b/g) wireless transmission modes.
8. Bidder shall describe the pros and cons of including Bluetooth wireless communications within the device.
9. The MID device shall be capable of communicating directly with a local printer, as well as remotely to a network printer.
    9.1. Bidder shall specify how communications with a local and network printer are accomplished.
10. Bidder shall describe what COTS operating systems are available to operate on bidder's device
11. SFPD contemplates SFPD/SFGOV may require or desire additional mobile applications operate on the MID device (e.g. mobile public safety software that interoperates with CAD/RMS/JMS/CLETS/NLETS/etc.)
    11.1.   Bidder shall describe any limitations of the device that prevent or impede the operation of third party and custom-built mobile applications (thick, thin and smart client) on the bidder's MID device
12. Bidder shall specify any and all COTS and proprietary drivers, middleware, development tools and applications offered by bidder for the device
13. The MID device shall be capable of establishing communications with the SFPD ABIS and initiating a centralized search of the SFPD ABIS and receive and display corresponding search results back from the ABIS and any other SFPD/SFGOV new or legacy systems.
    13.1.   The bidder shall describe how one, two, four or even ten fingers can be used for the search, including accommodating for missing or unusable fingers.
    13.2.   Bidder shall provide auto capture for the device and specify what parameters are automatically being checked and adjusted to obtain the best quality image (e.g. gain, contrast, brightness, finger detect, core detect and positioning, ridge presence, surface area of image, etc.).
        13.2.1. MID device shall allow the operator to override minimum image quality measurements as established by an administrator or operator
14. Bidder shall describe bidder's ability to utilize smart client software such that any and all updates for the software can be pushed down from a management server
    14.1.   This should include global changes to default software configurations and settings such as image quality thresholds, match thresholds, etc.
15. Application Access Controls and Security
    15.1.   Bidder shall describe how proposed MID solution complies with SFPD/SFGOV, CalDOJ/CLETS and FBI CJIS stipulated security and access control standards, requirements, certifications, guidelines and best-practices (e.g. multi-factor authentication of user/operator)
    15.2.   Bidder shall discuss their ability to support Citrix for access control to the MID workstation and application

15.3.   Bidder shall describe the proposed security architecture for the MID system and how data is protected throughout the transaction.

15.4.   Bidder shall describe if fingerprint images captured on the device are compressed with certified WSQ or JPG2000 compression algorithms.

16. Bidder shall indicate whether the application is a secure graphical user interface built on a thick client, thin client or smart client architecture (e.g. web application)

16.1.   Bidder shall describe required workflow and priority support to identify/verify individuals (suspects, persons of interest, known criminals, etc.) against the central ABIS and/or a local watchlist

16.2.   Bidder shall discuss their ability to leverage a COTS application server, workflow server and database server procured by SFPD via CLIN 4 to develop and deliver the application, including if CLIN 4 is procured from a different vendor than for this CLIN (CLIN 9).

16.3.   Bidder shall indicate whether existing Identix store-and-forward servers can be / will be used for the MID device to communicate with the ABIS and to receive results back (either via store-and-forward server or via separate server functionality)

17. SFPD recognizes the wide range in the quality of images from affordable fingerprint scanners, including the size of platens and FBI certification status.[30] SFPD also recognizes the difficulty in obtaining high accuracies with plain impression fingerprints without utilizing multiple fingers.

17.1.   Bidder shall describe why a particular vendor and model of fingerprint device is recommended (e.g. embedded in bidder's device), including benefits, risks and key pros and cons of utilizing said device.

18. SFPD also recognizes the value of fusing facial recognition into the MID application under the right lighting conditions and if the software application and process remains easy to implement and use.

18.1.   Bidder is encouraged to discuss the option of leveraging the planned FRS (see CLIN 8) and how bidder would fuse the results from the AFIS and FRS to ensure the overall accuracy of the match results remains high.

18.2.   Bidder shall describe why a particular vendor and model of digital camera is recommended (e.g. embedded in bidder's device), including benefits, risks and key pros and cons of utilizing said device.

19. SFPD recognizes the future value of fusing iris recognition into the MID application under the right lighting conditions and if the software application and process remains easy to implement and use.

19.1.   Bidder shall describe if the device can support the capture of iris images now or in the future.

---

[30] http://www.fbi.gov/hq/cjisd/iafis/cert.htm - Identification Flats Systems and PIV Single Finger Capture Devices

20. Bidder shall describe if the device can encode (extract) fingerprint templates on the device.

21. Bidder shall describe if the device can support on-board verification and identification (1:some) for one or more biometric modalities (finger, face or iris).

22. SFPD recognizes the future value of a device that can capture (dusted/enhanced) latent fingerprint and latent palmprint images from standard flat surfaces in the field (e.g. at a crime scene). Bidder shall describe if the device can be used to capture said latent prints now or in the future.

23. Bidder shall describe the pros and cons of the following OPTIONAL specifications for the MID device and how bidder's device can accommodate these options now or in the future:

    23.1.   OPTIONAL: A digital camera with the ability to capture medium/high resolution images (at least 90 pixels between the eyes when captured approximately 2 to 5 feet from the subject) to in any lighting condition (e.g. via a built-in flash, light, etc.)

    23.2.   OPTIONAL: A magnetic stripe reader capable of reading both legacy and REAL ID driver licenses now or in the future

    23.3.   OPTIONAL: A 1D/2D barcode reader capable of reading both legacy and REAL ID driver licenses now or in the future

    23.4.   OPTIONAL: A contactless/RFID reader capable of reading both legacy and REAL ID driver licenses now or in the future

    23.5.   OPTIONAL: A contact / contactless smart card reader capable of reading ANSI/NIST/ISO/IEEE compliant smart cards, including smart cards that adhere to the NIST FIPS 201 standard and the yet-to-be-published ISO/IEEE version of FIPS 201.

4.10.3 STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

2. MID device shall include an FBI certified fingerprint capture device

3. Bidder shall describe any and all compliance with US, International and/or military standards for drop testing, ruggedness, resistance to dust, liquids, etc.

4. MID device shall comply and/or be certified with the following US and international standards, certifications, best practices, etc. with respect to electrical/electronic devices. Bidder shall submit evidence of certification/compliance.

    4.1. FCC Part 15

    4.2. UL

    4.3. Bidder shall indicate any similar international compliances and certifications such as CE, Canadian ICES, etc.

5. Bidder shall describe MID system's ability to integrate into a Web 2.0 compliant SOA/ESB architecture

6. Application Access Controls and Security

6.1. Bidder shall describe how MID system complies with SFPD/SFGOV, CalDOJ and FBI CJIS stipulated security and access control standards, requirements, certifications, guidelines and best-practices

    6.1.1. Bidder shall describe the ability to support Citrix on MID device

6.2. Bidder shall describe how MID solution complies with NIST Information Access Division Image Group - Mobile ID Device Best Practice Recommendation

6.3. Bidder shall describe how MID device and software comply with open architecture principles

4.10.4 SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

2. Bidder shall install a total of ten (10) devices at various locations throughout SFPD including but not limited to:

    2.1. SFO Airport Bureau (on person, on Segway, in vehicle, etc.)

    2.2. Traffic Bureau (on person, on motorcycle, in vehicle, etc.)

    2.3. Other Units (on person, on bicycle, in vehicle, etc.)

3. Bidder shall provide wireless communications via cellular modem connection (e.g. 2G/3G) for the duration of the pilot, including all modem hardware and data services

    3.1. SFPD will work with bidder to ensure the lowest cost is available for modem hardware and data services leveraging government and law enforcement discount rates via a month-to-month contract

    3.2. SFPD will work with bidder to transition, augment or replace wireless data services to SFPD at the conclusion of the pilot in case SFPD desires to continue connectively and operations beyond the end of the pilot

4.10.5 SYSTEM OPERATION

1. See **System Operation** under **General Requirements**

2. At a minimum, bidder shall provide two (2) roaming support persons and two (2) vehicles for the first five (5) days of operations.

    2.1. Roaming support persons will move throughout the San Francisco area to each location where systems are installed on a standard routing schedule, breaking off the schedule only if a call for support arises to drive directly to the location where the support call came in from.

    2.2. One roaming support person will work a ten (10) hour shift from 0800 to 1800.

    2.3. The second roaming individual will operate a ten (10) hour shift from 1800 overnight to 0400.

    2.4. Either support person should be on-call from 0400 to 0800 in case a support request comes in.

4.10.6 SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**
2. Bidder shall demonstrate secure logon to the application as an administrator
3. Bidder shall demonstrate all administrator settings
4. Bidder shall demonstrate logoff the application
5. Bidder shall demonstrate secure logon to the application as a user
6. Bidder shall demonstrate all user-adjustable settings
7. Bidder shall demonstrate the capture of fingerprints (and photo) from an individual (test record)
8. Bidder shall demonstrate the launching of a lights-out search (fingerprint or fingerprint + face)
9. Bidder shall demonstrate the displaying of all available results to the screen, to include:
   9.1. Simple 'Red Light' / 'Green Light' response representing criminal history status
       9.1.1. OPTIONAL: Include wants and warrants status in the 'Red Light' / 'Green Light' decision logic
           9.1.1.1.   May require interface to existing or legacy systems such as CABLE/RMS/JMS system…bidder shall discuss this option and indicate level of effort
   9.2. Display of the SF# for the person (received from AFIS/ABIS system)
   9.3. Display of the most grievous crime the individual has been arrested for in the past (type of crime) (received from AFIS/ABIS system)
   9.4. OPTIONAL: Display of whether or not the individual is a sex offender or a juvenile
       9.4.1. May require interface to existing or legacy systems such as CABLE/RMS/JMS system…bidder shall discuss this option and indicate level of effort
   9.5. OPTIONAL: A black and white or color photo of the individual from the most recent booking
       9.5.1. Bidder shall indicate if bidder's MID device's screen remains small enough to make the overall device smaller in size while still possessing the ability to display a reasonable quality black and white or color photo
10. Bidder shall demonstrate the entering of a person's name
11. Bidder shall demonstrate the launching of a filtered search based on person's claimed name
12. See Number 9
13. Bidder shall demonstrate the entering of a person's SF#
14. Bidder shall demonstrate the launching of a filtered search based on SF#
15. See Number 9
16. Bidder shall logoff the application.

4.10.7 TRAINING

1. See **Training** under **General Requirements**
2. Bidder shall train students on how to capture plain impression fingerprints properly, including

     2.1. positioning of the finger

     2.2. amount of pressure and how to detect under and over pressure

     2.3. how to deal with dry or overly moist fingers

     2.4. how to deal with missing or overly damaged fingers

     2.5. how to deal with other exceptions (e.g. tattoos on finger surface, etc.)

     2.6. what a good fingerprint looks like

     2.7. how and when to override automatic image capture and quality checks for "best effort" searching

3. Bidder shall train students on how to routinely calibrate, clean and maintain the fingerprint device

4. Bidder shall train students on how to deal with and overcome wired and wireless communications errors

5. Bidder shall train students on how to capture photographs properly for purposes of searching FRS, if applicable to bidder's proposal, including

     5.1. positioning of the face

     5.2. lighting issues and how to overcome them

     5.3. how to deal with glasses

     5.4. how to deal with other exceptions (e.g. tattoos on face, etc.)

     5.5. what a good photo of the face looks like

     5.6. how and when to override automatic image capture and quality checks for "best effort" searching

6. Bidder shall train students on how to routinely clean and maintain digital camera (e.g. lens), if applicable to bidder's proposal

4.10.8 SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**

2. Bidder shall provide a brief description (with options) of the hardware warranty for the fingerprint devices.

4.11 CLIN 10 – NIST/NIJ LATENT INTEROPERABILITY

4.11.1 SCOPE OF IMPLEMENTATION AND OPERATION

See **Scope of Implementation and Operation** under **General Requirements.**

The National Institute of Justice (NIJ) is partnering with the National Institute of Standards and Technology (NIST) Office of Law Enforcement Standards (OLES) and has formed the AFIS Interoperability Working Group. The group has produced the overview of Information Sharing Mandates (i.e., relevant statutes, executive orders and Presidential guidance) that provide and facilitate the means for sharing information among all appropriate Federal, State, local, tribal, private sector, and foreign partners.

The Information Sharing Environment (http://www.ise.gov/pages/vision.html) mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. Section 1016 of the law required the President to designate a Program Manager for the ISE and establish an Information Sharing Council to advise the President and the Program Manager.

The working group has started the task of developing the Model Procurement Specifications. The high light of the draft is outlined below, as a reference will be the model SFPD will follow for this CLIN and procurement.

4.11.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**
2. Searches
3. The proposed system must be capable of receiving, processing, and responding to latent print searches generated from other devices or systems that utilize national standards for the exchange of latent print information. Additionally, the proposed system must be able to export native latent searches into the national standard format to be searched against other Automated Fingerprint Identification Systems. The following types of transactions are national standards that are documented in the FBI Electronic Biometric Transmission Specification (ANSI/NIST ITL 1-2007 or higher / EBTS version 8.1 or higher) and constitute the minimum required transactions. Vendors may provide additional functionality in their proposal.
    3.1. Submission Transactions
        3.1.1. LFFS - Latent Fingerprint Feature Search
        3.1.2. LFIS - Latent Fingerprint Image(s) Search
        3.1.3. LPFS – Latent Palmprint Feature Search
        3.1.4. IRQ – Image Request Query
4. Responses
    4.1. The proposed system must be able to generate responses to latent searches from other devices or systems in a manner that is compliant with national standards. The response standards are documented in the FBI Electronic Biometric Transmission Specification (ANSI/NIST ITL 1-2007 or higher/ EBTS version 8.1 or higher link to http://www.fbibiospecs.org/fbibiometric/biospecs.html) and constitute the minimum transaction specifications.
        4.1.1. Response Transactions
            4.1.1.1.   SRL - Search Result – Latent
            4.1.1.2.   ERRL – Transaction Error
            4.1.1.3.   IRR – Image Request Response
5. System Access
    5.1. The vendor shall provide an interface that is compliant with host agency network and computer security policies.
6. OPTIONAL: Vendors shall describe additional functionality in their CLIN 10 proposal (or using the optional add-on CLINS 11 to 14), including, but not limited to:
    6.1. Latent queue management designed to manage and prioritize externally generated searches
    6.2. The ability to retain/enroll unsolved latents generated by and submitted from other devices or systems.

6.3. Generation of a notification to the submitter in the event of an unsolved latent match. Notification format should be compliant with national standard. (ULM- Unsolved Latent Match)

6.4. Tracking: A methodology to collect the Hit/No Hit status on the SRL's. Similar methods have been used via e-mail to request a status x days after the SRL was provided. This can be completed by clicking on one of two links or other similar methods.

4.11.3 STANDARDS COMPLIANCE

1. See **Standards Compliance** under **General Requirements**.

4.11.4 SYSTEM INSTALLATION

1. See **System Installation** under **General Requirements**.

4.11.5 SYSTEM OPERATION

1. See **System Operation** under **General Requirements**

4.11.6 SYSTEM ACCEPTANCE

1. See **System Acceptance** under **General Requirements**.

4.11.7 TRAINING

1. See **Training** under **General Requirements**.

4.11.8 SUPPORT AND MAINTENANCE

1. See **Support and Maintenance** under **General Requirements**.

4.12 CLIN 11 TO 14 - CUSTOMIZATIONS, ENHANCEMENTS, EXPANSIONS

4.12.1 SCOPE OF IMPLEMENTATION AND OPERATION

See **Scope of Implementation and Operation** under **General Requirements.**

This CLIN delivers any OPTIONAL customization, enhancement and expansion on any other previously described CLIN as proposed by the bidder. The bidder is to propose one, two or up to four incremental hardware or software system customizations, enhancement or expansions (e.g. added functionality) not outlined in the Scope of Implementation and Operation or Mandatory Requirements in the corresponding CLIN.

4.12.2 SYSTEM FEATURES AND FUNCTIONS

1. See **System Features and Functions** under **General Requirements**.
2. See each corresponding CLIN for any OPTIONAL requirements that bidder may want to address in CLIN 11 through 14

CLIN 11 through 14 are completely optional and there are no specific requirements. Vendors are encouraged to provide specific information, requirements and benefits regarding any proposed features, functions or interfaces proposed by the bidder.

4.12.3 STANDARDS COMPLIANCE
1. See **Standards Compliance** under **General Requirements**.

4.12.4 SYSTEM INSTALLATION
1. See **System Installation** under **General Requirements**.

4.12.5 SYSTEM OPERATION
1. See **System Operation** under **General Requirements**.

4.12.6 SYSTEM ACCEPTANCE
1. See **System Acceptance** under **General Requirements**.

4.12.7 TRAINING
1. See **Training** under **General Requirements**.

4.12.8 SUPPORT AND MAINTENANCE
1. See **Support and Maintenance** under **General Requirements**.

5   APPENDIX A – LIST OF ABBREVIATIONS

ABIS	Automated Biometrics Identification System
AFIS	Automated Fingerprint Identification System
CABLE	California-Bay Area Law Enforcement system
CAL-DOJ	Or CalDoj; California Department of Justice

CalPhoto	California
CIO	Chief information Officer
CLETS	California Law Enforcement Telecommunications System
CMS	Court Management System
CODIS	Combined DNA Index System; the DNA database developed by the FBI to store DNA Profiles created by federal, state, and local crime laboratories in the United States, with the ability to search the database to identify suspects in crimes
COIT	Committee on Information Technology
CSI	Crime Scene Investigation
DA	District Attorney
DAI	District Attorney Investigation
DL	Driver License
DMV	Department of Motor Vehicle
DTIS	Department of Telecommunication and Information Services
EPEAT	Electronic Product Environmental Assessment Tool
FI	Field Interrogation
FMS	Forensic Case Management System
FOB	Field Operations Bureau

FSD	Forensic Services Division
GTF	Gang Task Force
IAFIS	Integrated Automated Fingerprint Identification System; The FBI AFIS housed in Clarksburg West Virginia.
ICT	Information and Communication Technology
JMS	Jail Management System
MEO	Medical Examiner Office
NCIC	National Crime Information Center
NGI	Next Generation Identification, the FBI ABIS under development now to replace the IAFIS.
NIBIN	National Integrated Ballistic Identification Network; a Branch in the Firearms Programs Division of the Bureau of Alcohol, Tobacco, Firearms and Explosives which provides Integrated Ballistic Identification System (IBIS) equipment into Federal, State and local law enforcement agencies for their use in imaging and comparing crime gun evidence.
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunication System; It is the interstate law enforcement network in the nation for the exchange of law enforcement and related justice information
PID	Positive ID (PID) devices; added in order to provide an automated pre-booking / intake identification capability at the city's district police stations and county jail
RFI	Request for Information
RFP	Request for Proposal

RFQ	Request for Quote
RMS	Record Management System
S&F	Store & Forward
SF #	San Francisco Number
SFDAO	San Francisco District Attorney Office
SFO #	San Francisco Airport Number
SFPD	San Francisco Police Department
SFSD	San Francisco Sheriff Department
TCN	Transaction Control Number
TP	Tenprint (fingerprint)
ULF	Unsolved Latent File
USL	Unsolved Latent
VCIN	Violent Crime Information Network
RDBT	Existing NEC AFIS solution
Palm-DB	Palm Database
LDB	Latent Database – Fingerprints
LDB-P	Latent Database – Palmprints

TI	Tenprint Input
LI	Latent Input

6   APPENDIX B – ABIS METRICS

6.1   EXISTING AFIS DATABASE PERSON-RECORD GROWTH RATES BY SEX

Date	Male	No of Record Increase	Percentage Increase
12/26/04	340,342		
12/25/05	348,488	8,146	2.39%
12/31/06	356,786	8,298	2.38%
11/25/07	365,259	8,473	2.37%

Date	Female	No of Record Increase	Percentage Increase
12/26/04	87,337		
12/25/05	90,080	2,743	3.14%
12/31/06	92,916	2,836	3.15%
11/25/07	95,529	2,613	2.81%

Date	Unknown	No of Record Increase	Percentage Increase
12/26/04	142		
12/25/05	161	19	13.38%
12/31/06	230	69	42.86%
11/25/07	267	37	16.09%

Date	Male/Female/ Unknown Total	No of Record Increase	Percentage Increase
12/26/04	427,821		
12/25/05	438,729	10,908	2.55%
12/31/06	449,932	11,203	2.55%
11/25/07	461,055	11,123	2.47%

6.2   AFIS TRANSACTION COUNTS BY TYPE

The zero entries indicate no-report and are not used in the average calculations.

	Tenprint Daily Transactions in a Month		Latent Daily Transactions in a Month	
	2005	**2007**	**2005**	**2007**

January	116.5	97.0	19.6	13.3
February	0.0	113.0	0.0	18.6
March	121.0	110.0	20.7	16.9
April	124.5	113.3	16.5	15.8
May	0.0	116.1	0.0	17.5
June	115.7	118.0	13.0	15.4
July	102.8	108.0	14.8	16.0
August	112.4	109.0	13.3	12.0
September	112.4	114.0	13.3	17.0
October	104.7	114.0	13.3	14.0
November	106.1	0.0	17.5	0.0
December	0.0	0.0	0.0	0.0
Average	**112.9**	**111.2**	**15.8**	**15.7**

6.3   EXISTING AFIS SYSTEM CAPACITY

As of the March 2009 system report, the AFIS had:

RDBT	Palm-DB	LDB	LDB-P	Archive TCN Number
475,634	165,472	10,647	457	777,014

6.4   PROJECTED FIXED POST ID TRANSACTION VOLUME

SFPD projects the following transaction volumes for the approximately 30 Fixed Post ID (FPID) applications under normal operating conditions:

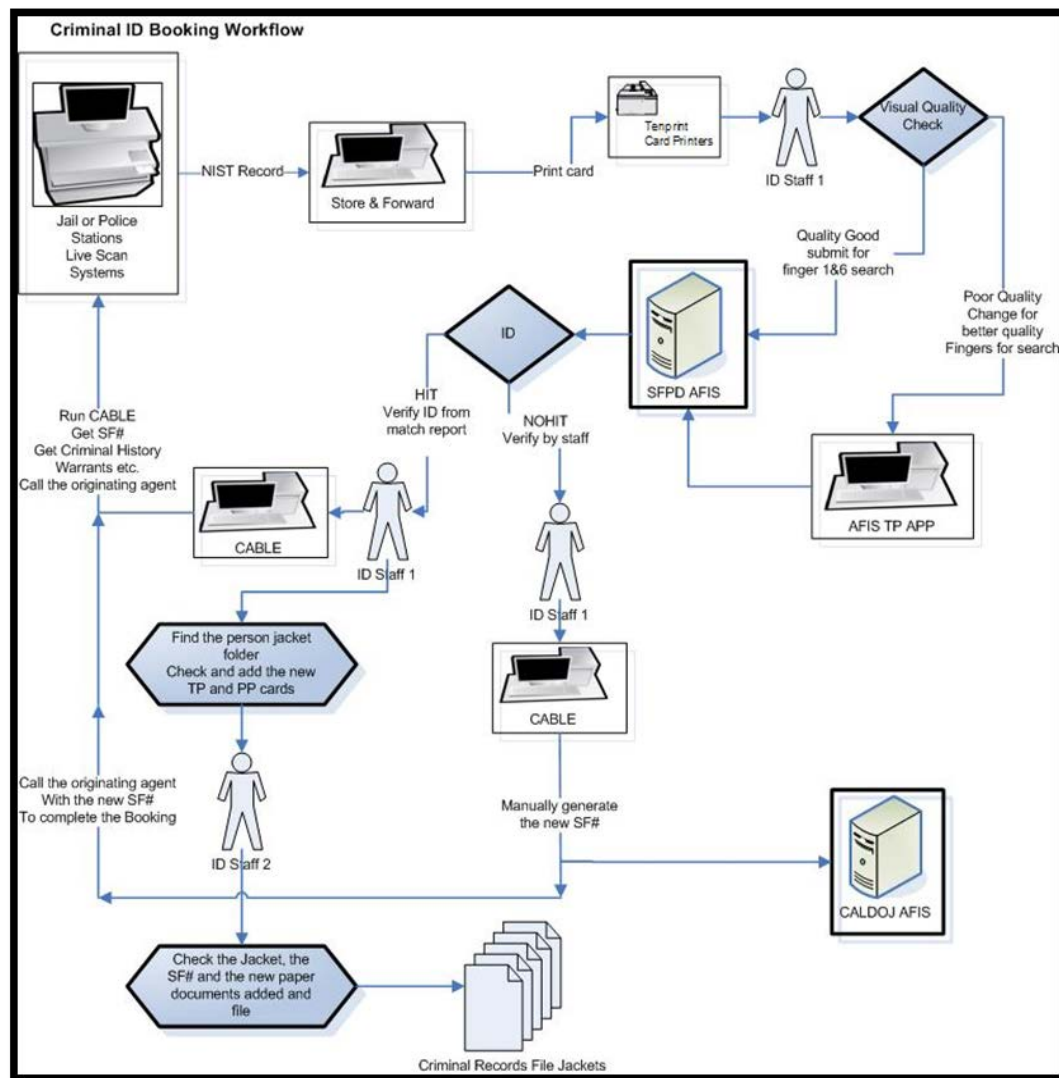| Average Volume of Identifications (Per Hour)	Peak Volume of Identifications (Per Hour)	Maximum Response Time Allowed for Identification (Minutes)	Average Volume of Verifications (Per Hour)	Peak Volume of Verifications (Per Hour)	Maximum Response Time Allowed for Verification (Minutes)
4 x 30 = 120	8 x 30 = 240	2	8 x 30 = 240	12 x 30 = 360	0.25

6.5   PROJECTED MOBILE ID TRANSACTION VOLUME

SFPD projects the following transaction volumes for the Mobile ID (MID) application during the pilot project (10 devices).

Average Volume of Identifications (Per Hour)	Peak Volume of Identifications (Per Hour)	Maximum Response Time Allowed for Identification (Minutes)	Average Volume of Verifications (Per Hour)	Peak Volume of Verifications (Per Hour)	Maximum Response Time Allowed for Verification (Minutes)
4 x 10 = 40	8 x 10 = 80	2	8 x 10 = 80	12 x 10 = 120	0.25

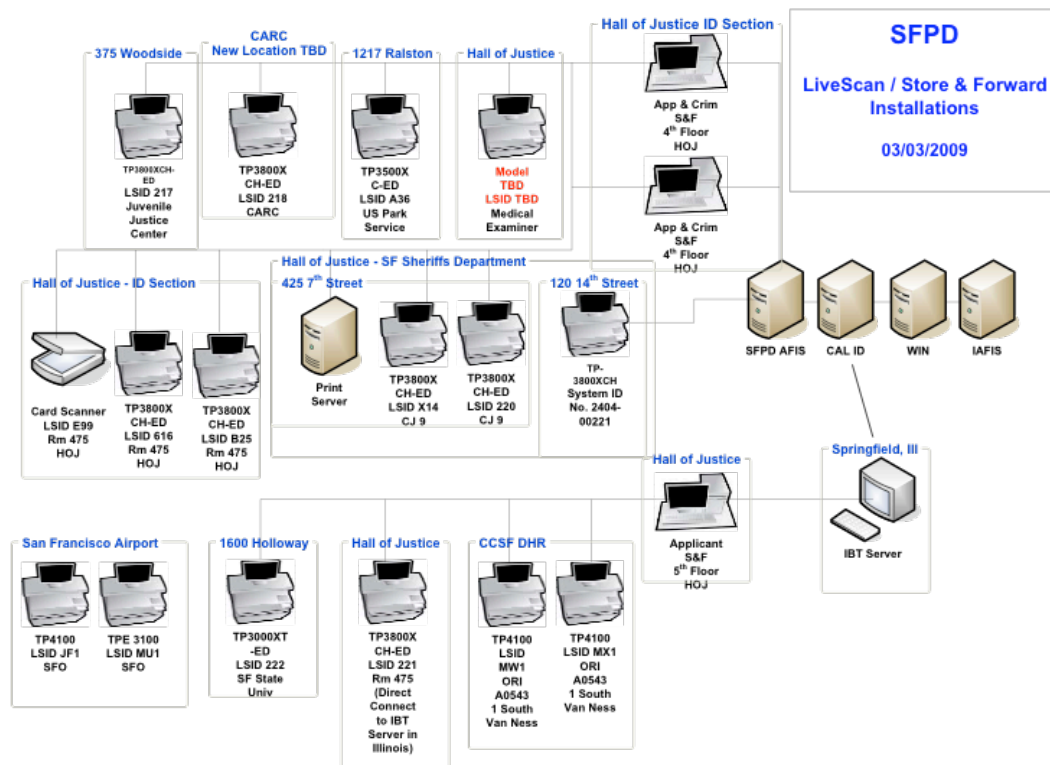## 7   APPENDIX C – DIAGRAMS AND WORKFLOWS

7.1   CURRENT CRIMINAL BOOKING WORKFLOW
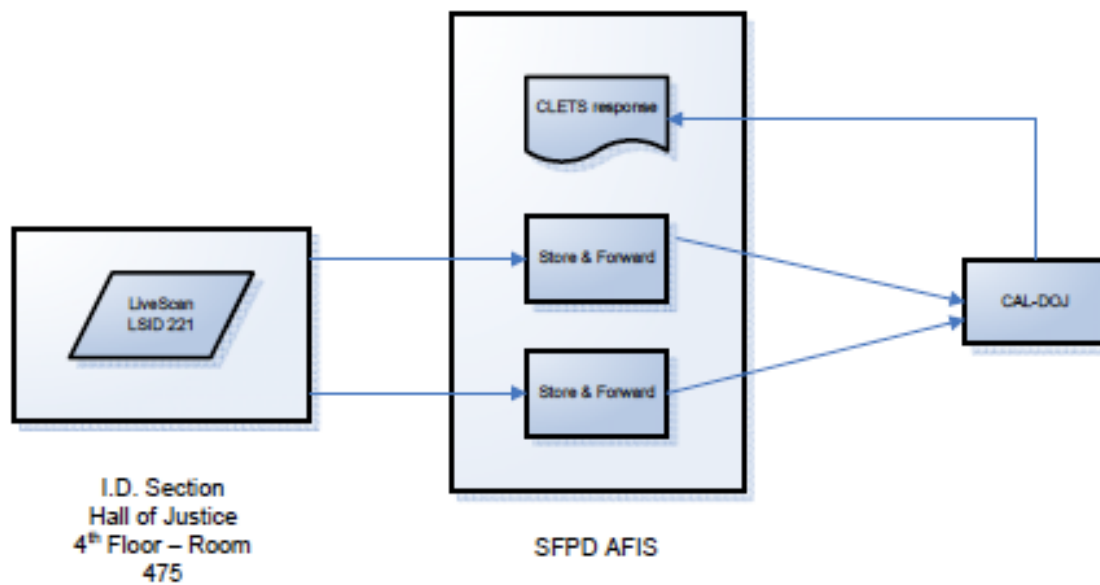
7.2   CURRENT CRIMINAL WORKFLOW
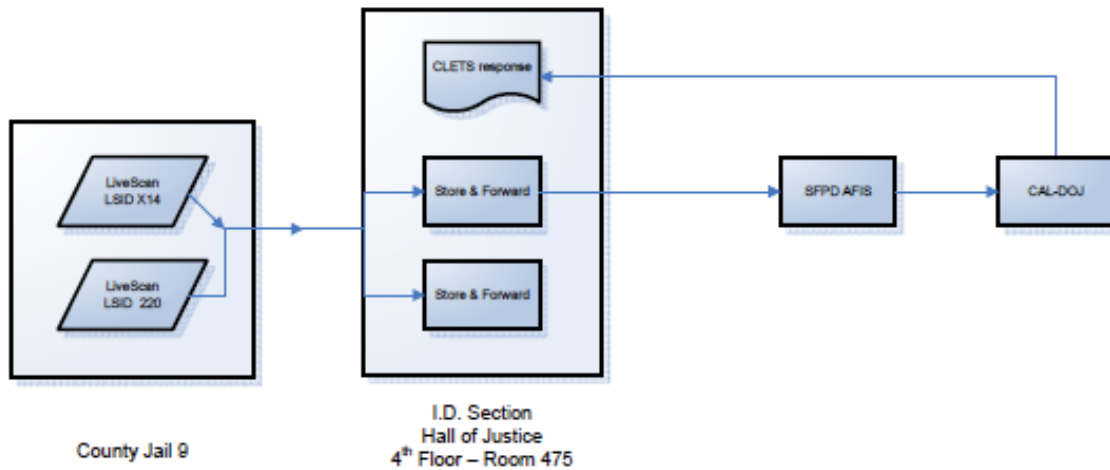
7.3 CURRENT APPLICANT WORKFLOW DIAGRAM

7.4   CURRENT REGISTRANT WORKFLOW DIAGRAM

7.5   LATENT PRINT WORKFLOW DIAGRAM